

国际信息工程先进技术译丛



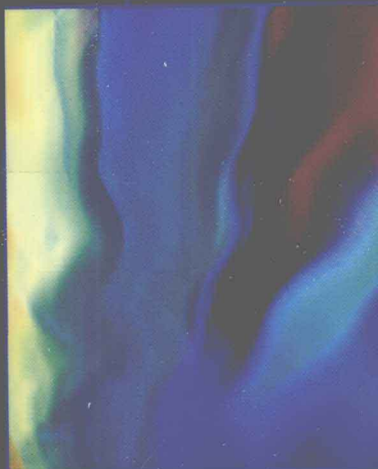
Springer

# WirelessHART：面向工业自动化的实时网状网络

# WirelessHART: Real-Time Mesh Network for Industrial Automation


Deji Chen
（美） Mark Nixon 著
Aloysius Mok

王泉 王平 韩松 译






机械工业出版社
CHINA MACHINE PRESS

国际信息工程先进技术译丛

# WirelessHART：面向工业自动化的实时网状网络

Deji Chen
（美）Mark Nixon 著
Aloysius Mok
王泉 王平 韩松 译



机械工业出版社

近年来，WirelessHART 的标准和技术受到了广泛关注，但是目前业内尚无该技术相关的指导性书籍。鉴于此，本书详细地介绍 WirelessHART 及无线工业自动化，是第一本关于 WirelessHART 工业控制应用的著作。通过阅读本书，工程师能更深入地掌握该技术，丰富其 WirelessHART 系统开发及产品开发经验；用户也能更全面地理解该技术及应用，有利于其在工业自动化领域采用该技术；向学术界介绍工业无线领域的潜在研究热点，有利于其拓展和提升学术研究成果。

本书理论框架严谨，内容新颖丰富、论述精辟、覆盖面广，注重理论与实际的有机结合，具有很强的可读性。既可以作为工业自动化、计算机应用、仪器测控和传感器技术等专业人员的参考书，也可以供广大对工业过程控制和无线技术感兴趣的工程技术人员参考。本书的出版必将对国内读者更深入地了解、掌握和使用 WirelessHART 系统以及工业无线技术起着重要的推动作用。

Translation from the English language edition:
WirelessHART™ Real-Time Mesh Network for Industrial Automation
Deji Chen, Mark Nixon, Aloysius Mok
ISBN: 978-1-4419-6046-7

本书版权登记号：图字 01-2011-1519 号

**图书在版编目（CIP）数据**

WirelessHART：面向工业自动化的实时网状网络／（美）陈德基，（美）尼克松（Nixon，M.）（美）莫（Mok，A.）著；王泉等译．—北京：机械工业出版社，2012.11
（国际信息工程先进技术译丛）
书名原文：WirelessHART：Real-Time Mesh Network for Industrial Automation
ISBN 978－7－111－40815－4

Ⅰ.①W…　Ⅱ.①陈…②尼…③莫…④王…　Ⅲ.①工业自动控制－无线网　Ⅳ.①TP273

中国版本图书馆 CIP 数据核字（2012）第 304215 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）
策划编辑：林　桢　责任编辑：林　桢　责任校对：肖　琳
封面设计：马精明　责任印制：张　楠
北京京丰印刷厂印刷
2013 年 1 月第 1 版第 1 次印刷
169mm×239mm · 15.75 印张 · 388 千字
0 001—3 000 册
标准书号：ISBN 978－7－111－40815－4
定价：80.00 元

# 原书前言

过程控制工业已经历了数代技术革新，从气动通信发展到电气通信再到电子通信，从集中式控制发展到分布式控制。现如今，操作站位于分布式控制系统的中心，在过程控制系统中的工业监视器与执行器之间提供通信服务。随着新一代产品的出现，操作站更加趋于智能化。依托于智能现场设备，最新的应用程序能提供更加完备的报警、控制及故障检测服务。这些智能现场设备能提供更全面的过程信息，能降低工程造价，还能有利于改善整个工厂的操作性能。智能设备通常包含有高级故障诊断功能，该高级故障诊断功能可以报告设备的健康状况，并且在许多情况下能够反映出与该设备相连的工业过程的健康状况。智能现场设备的故障诊断功能通常包括检测管道堵塞、燃烧器火焰的不稳定性、搅拌器的损耗、湿气、孔的磨损、泄漏、气蚀等。这些智能现场设备还可以向用户报告设备本身的运行状况以及设备何时需要维护。随着传感器和故障诊断技术的发展，各式各样的智能现场设备纷纷涌现。然而，随之而来的问题是：用户怎么才能将智能现场设备的最新功能与现有控制系统的基础设施连接起来呢?

答案是无线技术。无线技术已发展成为一项较为成熟的技术，现在可以被安全地应用于工业控制、监测、资产管理等领域。它为传统控制系统提供了一种高性价比的替代通信方式，用以访问现场设备中的智能信息。以往高成本的测量现在可以由无线技术实现并融入到监控系统中。无线技术以高性价比、简单、可靠的方式实现测量和控制，没有架设线路的开销，也不需要彻底改变现有系统。无线技术还能为中央控制器和移动用户提供有效的平台，以便它们来访问工业过程及过程设备。

工业过程控制急需无线技术的全球性标准，以便不同设备厂商制造的设备能够彼此协同工作，这样能够降低供应商和用户双方的风险和成本。有着独一无二地位的 HART 通信基金会制定了一种这样的标准。

自 1989 年以来，HART 通信协议作为世界领先的过程通信技术，一直为智能仪表提供服务。工业产品供应商以创纪录的数量制造 HART 产品。世界范围内，安装和运行着的 HART 产品超过了 3 千万台。在已安装的智能仪表中，75% 的仪表是基于 HART 标准的。

然而，对于大约 85% 的 HART 智能仪表，只有过程变量数据以 4 ~ 20mA 模拟信号的方式被传送着，仪表内部大量的其他数据没有被故障诊断应用访问，从而滞留于设备中。这往往是由于访问这些内部数据的成本过高、难度过大。

经过数十年的发展，HART 通信基金会及其 230 个加盟成员公司找到了一种满

足过程工业特殊要求的无线技术标准。依托成员公司的技术资源和专业技术优势，HART通信基金会创造出了一种全新的无线技术。这种新的无线技术在拓展HART协议功能的同时，也充分考虑了全球范围内已有大量HART设备被安装的现实。在最新的增强版HART标准中，HART通信基金会吸收了一些经过应用验证的现场通信技术、网络技术和安全协议，并将其整合成简单、可靠、安全的无线技术标准。

**WirelessHART技术的简便性**

WirelessHART是一种易于实现的、可靠的技术。通过与现有HART设备、工具和系统兼容，它可以提供与HART产品相关的安全、简便、可靠的用户体验。正因如此，有过HART产品使用经历的用户都能够简单、快速地感受到WirelessHART技术的优势。

WirelessHART技术的简便性一方面源于WirelessHART网络的自身特性。WirelessHART网络是一种自组织、可自愈、自适应的网络，它能自动调整以适应工厂环境的变化（例如新设备连接到网络时引起的变化）。

WirelessHART技术的简便性还源于无线技术的自身特点。线缆架设和材料开支的减少，使设备的安装和调试过程更加简单，这样就降低了人力成本。摆脱了架设线缆的束缚，网络可以很方便地覆盖至偏远地区。网络的构建可以以每次布置一个设备的方式来实现，而不需要一开始就构建出整个系统。

与有线HART设备的良好兼容，使得有线HART设备和WirelessHART设备能共存于同一系统中，同时还能将WirelessHART系统无缝地整合到已有的上位机、集散控制系统以及资产管理应用程序中。

WirelessHART技术的其他优势还包括可以减少工程项目成本和时间。用户可以简单、快速地通过WirelessHART网络来获取一些额外的测量数据，从而避免了人工收集数据，并且监控范围还可以拓展至一些偏远的工矿地区（例如油罐区、公共设施等）。有了这些额外的测量数据和诊断信息后，用户就可以实现回路故障的检修、简化维护过程，并且能够实现更广范围的检修时间预判。无线技术还可用来帮助检测对规范（例如健康、安全和环境规范）的遵守情况。

WirelessHART还具有一些其他的优势。由于没有线缆的限制，WirelessHART设备可以被架设在运动的设备（例如轨道车）和平稳转动的设备（例如窑炉）上。这些无线设备可以像传统有线设备一样与主控系统通信。采用无线技术还能更简单、更快捷地构建出一个用于过程研究的临时系统。

**WirelessHART技术的可靠性**

WirelessHART技术的许多特性保证其在工业环境中也能提供可靠的数据通信，而这些工业环境通常是很不利于无线通信的。工业环境通常由高密集度的铁制设施组成，而这些铁制设施会干扰无线信号的传输。此外，在工业环境中，大型设备常

会频繁地移动，现场条件也会不断地变化。各种各样的射频和电磁干扰都会影响通信的顺畅。WirelessHART 技术采用了直接序列扩频技术和跳频扩频技术来将通信分散到多个不同的物理信道。

WirelessHART 网络是一种冗余的、可自愈的网络。它是一种能支持多个接入点的网状网络，而非星形或树形拓扑结构的网络。它能检测到传输路径的恶化并自动修复，还可以自动选择路径从而绕过障碍物，还能随机地在不同信道上通信。WirelessHART 网络在其整个生命周期内都会不断地调整自己以适应环境的变化。这种自适应能力是利用网络设备不断发出的健康报告和诊断信息来实现的。

WirelessHART 网络具有的许多技术使得它能很好地与其他无线网络共存。这些其他无线网络可以是其他 WirelessHART 网络或者其他非 WirelessHART 网络。WirelessHART 网络在实际传输之前先对目标信道作信道空闲评估测试，那些时常受干扰或已被占用的信道将会被禁止使用。WirelessHART 网络中的报文传送是高度同步的，这样既能提供实时的报文传输，又能优化通信的带宽和调度。

**WirelessHART 技术的安全性**

WirelessHART 技术采用强健的安全措施来随时保障网络和数据的安全。这些安全措施包括了最先进的安全技术，从而能提供最高层次的安全保护。WirelessHART 技术在多个子层里都使用了工业标准的 128 位 AES 加密算法。数据链路层的网络密钥用于认证每次数据传输。在网络层，每个会话都有不同的密钥以加密和认证点对点通信。每个 WirelessHART 设备都拥有各自的加入密钥，用于设备入网过程中的加密和认证。此外，在网络的整个生命周期中，网络管理器会周期性地更换网络中所有的密钥。

WirelessHART 标准采用了多种技术来保护网状网络自身的安全。它在时隙层面上采用了跳信道技术，这样实际传输的物理信道在信息将要被传送时才被确定。设备的传输功率可由网络管理器控制。大功率传输可用于应对高噪声环境，而小功率传输可用于覆盖小区域的网络（例如用在生物反应器上）。此外，小功率传输往往使网络入侵者更难察觉到通信的相关信息。

WirelessHART 标准着眼于工业需求。它支持工业应用的所有环节，从快速工程设计、安装、试运行，到简单的故障诊断和排除以及可将计划内维护变成更合算的预见性维护。WirelessHART 标准正式发布于 2007 年 9 月，是第一个为过程自动化制定的、开放的、具有良好互操作性的无线通信标准。作为一种高性价比的技术，WirelessHART 能兼容当前已安装的 HART 设备，并且完全可以得到遵循 HART 标准的设备、工具和系统的支持。HART 标准除了考虑到过去及现在的 HART 设备，还确保现在的 HART 设备和未来的 HART 设备之间也能相互协调的工作。

# 序　一

物联网市场巨大，应用前景广阔。目前，世界各国都对物联网非常重视，美国提出的“智慧地球”战略以及我国提出的“感知中国”战略，其基础就是目前被广为推崇的“物联网”技术。有人预测，10年内“物联网”就有可能大规模普及，到2020年，世界上物物互联的业务，跟人与人通信的业务相比，将达到30:1，仅仅是在智能电网和机场防入侵系统方面的市场规模就有上千亿元。因此，“物联网”被称为是下一个万亿级的信息技术产业。

同时物联网的应用正蓬勃发展，向各个领域迅速渗透。由于无线通信技术的发展，通信的可靠性不断提高，设备成本不断降低，无线物联网技术成为该领域发展的一个主要方向。目前的物联网通信技术包括：电力载波、2G/3G/4G移动通信、RFID等技术，这些技术在单独用于传感网络的时候，分别存在可靠性较低、使用成本过高、通信距离过短等问题，WirelessHART作为第一个获得IEC（国际电工委员会）认证的工业无线网标准（IEC62591），其在可靠性/抗干扰性、安全性、组网灵活性和兼容性方面具备独特优势。

在过去的近三十年中，HART技术在工业自动化应用领域取得了骄人的成就。ARC Advisory Group最近的一份研究报告显示，至2010年底，共有约6900万台现场设备安装在全球各地，其中46%是HART设备。这使其在所有的现场通信协议中独占鳌头，甚至超过基于现场总线（含基金会现场总线、Profibus和其他数字通信协议）、专用协议和4~20mA（模拟/非智能）的所有设备总和。

而最为对HART技术进行扩充和增强的就是WirelessHART技术，它集成了可靠、稳定、成熟的IEEE 802.15.4的底层技术，采用先进的无线网络管理技术，引起了业界的广泛关注。

我们非常高兴看到本书的问世。中国在很多方面对全球高新科技的接受程度非常高。当今工业自动化上的技术革新提供给了中国从全球制造中心转变为“智造中心”的千载难逢的机会。HART通信基金会也希望将HART及WirelessHART技术更广泛和深入地在中国推广，帮助中国成为全球“智造中心”。

HART通信基金会亚洲区技术服务总监

冯翔　博士

2012年12月9日

# 序　二

我从事自动化及仪器仪表行业的科研和标准化工作已25年，其中经历了工业控制网络技术上的几次重大发展，从20世纪90年代的“现场总线大战”，到21世纪初兴起的工业以太网，再到现在的热点技术——工业无线技术。每次技术的创新与发展都会为产品供应商带来新的更大的市场，谁先推出产品，谁就先占领市场制高点，谁也往往成为最终的赢家。因此，所有大公司取得成功的经验是，不仅仅要紧跟技术发展的步伐，更要作为新技术的培育者，引领着本领域技术发展的方向。所以工业无线技术从一开始就引起了许多先进工业国家及国际自动化巨头公司的高度关注，纷纷投入巨资开展相关研发工作。WirelessHART就是其中一个很具有代表性和得到广泛认可的技术，也最先成为工业无线方面的IEC国际标准（IEC 62591：2010）。

WirelessHART得到Emerson、Siemens、ABB、E+H等公司的鼎力支持。据悉，目前在过程控制领域的PROFIBUS国际组织和现场总线基金会（Field bus Foundation）都不再推出自己的工业无线通信技术，而统一支持WirelessHART。这样无论从技术发展还是产品供应方面，都带给了市场和用户足够的信心。WirelessHART具有市场潜力的优势还在于它与原有有线HART仪表和控制系统完全兼容，只要是基于HART的设备、工具、应用软件和工作流程等都可继续保留使用，这无疑使得WirelessHART可借助广泛使用的HART设备而迅速拓展无线仪表市场。例如，Emerson公司去年在中国市场上的WirelessHART仪表和系统的销售与应用已经取得相当大的成绩。

作为全国工业过程测量和控制标准化技术委员会的秘书长，我于十多年前就开始了与HART通信基金会的接触。近年来，随着HART与WirelessHART技术产品在我国市场份额的迅速增长，HART通信基金会也越来越重视我国市场，终于在2010年年底与全国工业过程测量和控制标准化技术委员会合作，开始了HART和WirelessHART中国标准的转化，预计将于今年年底前成为中国标准。

本书的三位作者都是从事工业过程控制领域研究的资深专家，对WirelessHART技术和规范的开发以及IEC 62591标准的制定有着突出贡献。本书总结了WirelessHART技术的精华，它的问世恰好提前向读者给出了WirelessHART的技术概况，为工程师应用和开发WirelessHART产品提供指导。

我们期待着WirelessHART取得与有线HART一样的成功。

**机械工业仪器仪表综合技术经济研究所**

**所长　欧阳劲松**

# 序　三

工业过程自动化技术是当代发展最迅速、应用最广泛、效益最显著、最引人注目的关键技术之一，是推动新技术革命和新产业革命的关键技术之一，是电子信息技术的综合集成技术之一，也是走向新型工业化道路的关键技术之一。工业无线控制技术是当前工业自动化领域关注的热点之一。

由陈德基先生等合著、2010 年由 Springer 出版社出版的《WirelessHART™ Real-Time Mesh Network for Industrial Automation》英文版一书，经由王泉先生等将该书翻译成中文版呈现给广大工业自动化等行业的科技工作者，使其对了解工业过程控制无线技术一定受益匪浅。

WirelessHART 通信规范（HART7.1）于 2008 年 9 月 19 日正式获得国际电工委员会（IEC）的认可，成为一种公共可用的规范（IEC/PAS 62591Ed.1）。本书全面系统地介绍了 WirelessHART 作为第一个开放式的可互操作无线通信标准，能够满足流程工业对于实时工厂应用中的可靠、稳定和安全的无线通信的关键需求的内容。本书介绍了 WirelessHART 通信标准与已有国际标准的兼容情况，包括 HART 协议（IEC 61158）、EDDL（IEC 61804-3）、IEEE 802.15.4 无线电和跳频、扩频和网状网络等相关技术。深入浅出地介绍了 WirelessHART 网络的各组成部分：连接到过程或工厂设备的无线现场设备；使这些设备与连接到高速背板的主机应用程序或其他现有厂级通信网络能通信的网关，以及负责配置网络、调度设备间通信、管理报文路由和监视网络健康的网管软件；网管软件能和网关、主机应用程序或过程自动化控制器集成等内容。

本书的出版对于读者了解工业过程控制无线技术具有重要的实际意义，同时也具有现实的指导意义。本书理论框架严谨、内容新颖丰富、论述精辟、覆盖面广，注重理论与实际的有机结合，具有很强的可读性。既可以作为工业自动化、计算机应用、仪器测控和传感器技术等专业技术人员的参考书，也可以供广大对工业过程控制和无线技术感兴趣的工程技术人员参考。本书的出版必对国内读者更深入地了解、掌握和使用 WirelessHART 标准发挥重要的推动作用。

清华大学精密仪器与机械学系
教授　王雪
2012 年 11 月 5 日

# 目　　录



## 第一部分　WirelessHART 简介

# 第二部分 WirelessHART 深入

# 第三部分　WirelessHART实践



# 第四部分　WirelessHART展望

# 第一部分　WirelessHART 简介

该部分将整个 WirelessHART 标准简述为一个简短的小册子；在阅读完该部分后，读者被鼓励进一步阅读 WirelessHART 标准以获得更详细的知识。只有 HART 通信基金会的成员被给予获得 HART 标准。然而，WirelessHART 通信标准（HART 7.1）于 2008 年 9 月 19 日正式获得国际电工委员会（IEC）的认可，成为一种公共可用的标准（IEC/PAS 62591Ed. 1）。请访问 HART 通信基金会网站 http：//www. hartcomm. org 以获取更详细资料。

第 1 章介绍 HART 简史；

第 2 章介绍 WirelessHART 的物理层；

第 3 章介绍 WirelessHART 的数据链路层；

第 4 章介绍 WirelessHART 的网络层和传输层；

第 5 章介绍 WirelessHART 的应用层；

第 6 章概述整个 WirelessHART 网状网络。

用于描述协议栈内信息流的术语

| 包 术 语 | 包 的 含 义 |
|---|---|
| 请求（Request） | 上层发送请求给下层 |
| 确认（Confirm） | 下层回复“请求” |
| 指示（Indicate） | 下层发送一个请求给上层，大多数情况下包含一个来自于其他网络节点的新信息 |
| 响应（Respond） | 上层回复“指示” |

例如，节点 A 发送一个命令给节点 B，节点 B 会返还一个命令响应给节点 A。节点 A 发出的命令是一个请求（Request）包，该请求包将会在节点 A 的协议栈各层间向下传递，当该命令在节点 B 的协议栈各层间向上传递时可被理解为指示（Indicate）包；节点 B 回复的命令可被理解为响应（Respond）包，该响应包在节点 B 的协议栈各层间向下传递，当该命令在节点 A 的协议栈各层间向上传递时可被理解为指示（Indicate）包。在节点内部，当一个数据报被成功地发送出后，一个确认（Confirm）包将在协议栈各层间向上传递。

1. 协议栈各层间的交互

下层通常为上层提供一系列应用程序接口（Application Programming Interface，API）。这些应用程序接口被统称为服务原语（Service Primitive，SP）。从上层发送到下层的包是请求或者响应服务原语。从下层发送到上层的包是确认或指示服务原语。

服务原语可分为两个系列：管理服务原语和数据服务原语。数据服务原语是用于数据报的传送，管理服务原语用于协议栈各层的配置。

# 第1章 概　　述

摘要：本章简要概述 WirelessHART 标准。HART 标准已存在有二十多年，它拥有数量最多的已部署在世界上所有现场总线网络的现场设备。在 HART 标准的最新版本 7.0 中，WirelessHART 部分将无线技术应用到过程工业。WirelessHART 标准是工作于 2.4GHz ISM 频段的、安全的网络技术，它结合了基于 IEEE 802.15.4 的直接序列扩频（DSSS）射频技术与基于数据报的跳信道技术。WirelessHART 标准与 HART 标准共享同一个应用层，但 WirelessHART 标准拥有自己的网络层、数据链路层、物理层。1.3 节简要介绍 WirelessHART 的网络层、数据链路层、物理层。1.4 节列出了一个简单的 WirelessHART 应用案例。

## 1.1　关于 HART 标准

HART 标准（www.hartcomm.org）制定于20世纪80年代后期。在其最初版本中，HART 现场通信协议被叠加在一个 4～20mA 信号上以提供与智能现场仪表的双向通信，并且没有危害测量数据的完整性。在 HART 标准存在的 20 多年里，HART 协议从一个基于 4～20mA 的简单协议发展为当前无线和有线技术结合的协议，并拥有了许多新的特点，如支持安全、自发数据传输、事件通告、块模式传输和高级诊断等。目前，诊断信息包括有设备信息、设备附属装置的信息以及在某些情况下的实际监测过程。图 1-1 总结了 HART 标准的演变过程。

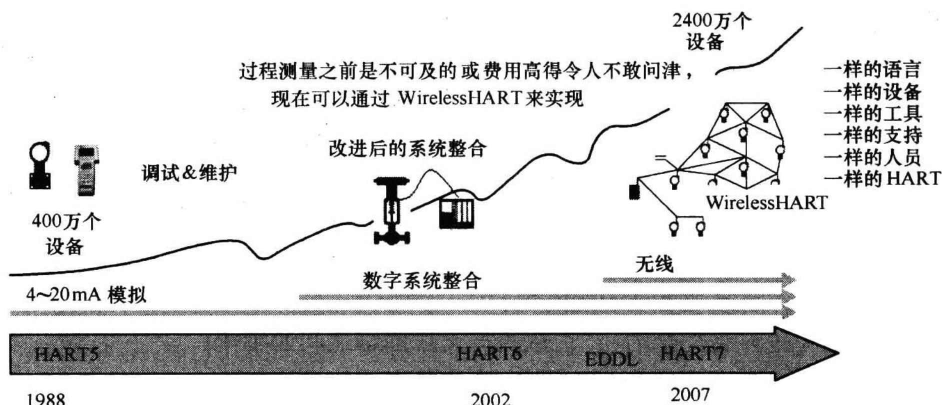



图 1-1　HART 标准的演变过程

HART 标准的最新版本（7.0 版）涵括了一些新特点，以改善系统的性能、增强诊断能力和提供更好的维护能力。这些新特点包括：

1）支持无线网状网络；

2）添加了时间同步和时间戳；

3）增强了报文的发布/订阅（突发模式）服务；

4）添加了传输层；

5）添加了网络层；

6）添加了高速文件传输管道；

7）添加了安全/加密/解密。

## 1.2 关于 WirelessHART 标准

为了支持无线应用，HART 7.0 版本包含了一个新的重要通信协议，即 WirelessHART 协议。像有线 HART 协议一样，WirelessHART 协议的应用对象是固定的传感器和执行器。WirelessHART 的目标市场还包括灵活的制造设备以及旋转装置（例如窑式干燥机）。WirelessHART 可用于保护用户已有以及新的投资。我们需要保护传统的产品及应用，继续现有的工作惯例及培训。我们也需要使用无线技术来降低测量成本、访问仪表内部的高级诊断信息以及拥有更好能力来监测设备。

WirelessHART 标准采用一些现有的标准，如 HART 标准、IEEE 802.15.4 标准、AES-128 加密标准，以及 DDL/EDDL 标准。有线 HART 能做到的，WirelessHART 标准都能做到并且可以做得更多。WirelessHART 标准是工作于 2.4GHz ISM 频段的安全网络技术，它结合了基于 IEEE 802.15.4 的直接序列扩频（DSSS）射频技术与基于数据报的跳信道技术。WirelessHART 网络支持来自众多制造商的各种各样的设备。图 1-2 描述了几种基本的网络设备类型，其中包括：

1）现场设备：实现现场感知或执行功能的基本设备；

2）现场路由设备：主要作为路由器而提供服务；

3）现场适配器：将有线 HART 设备连接到无线网状网络；

4）手持设备：被移动用户随身携带；

5）接入点：连接现场设备到网关；

6）网关（也许是冗余的）：上位机与无线网络之间的桥梁；

7）网络管理器（也许是冗余的）：也许驻留于网关设备中。

WirelessHART 网络通过使用一种被称为时分多址（TDMA）的方法来精确调度网络中的通信。WirelessHART 网络中的通信绝大多数都是沿着图路由方向的。集

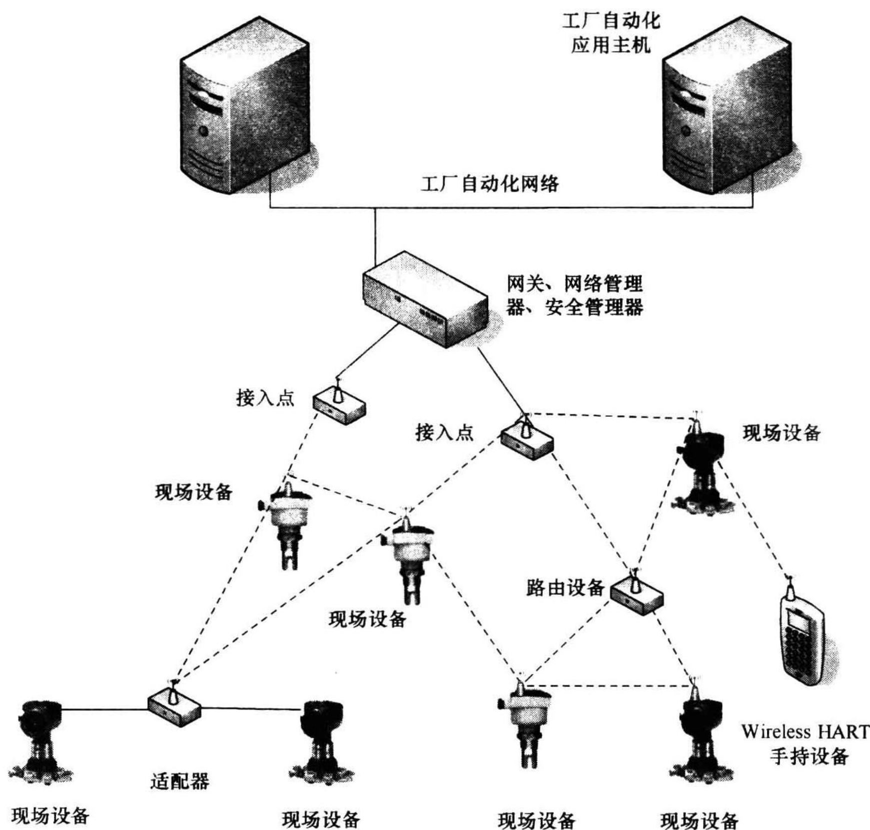



图 1-2 网络设备类型

中式网络管理器利用设备和应用程序提供的总体网络路由信息，并结合通信需求来实现对全网的调度和资源分配。通信时间被调度并分成许多个时隙，并由网络管理器传递给现场设备；现场设备只被提供了用以满足它们通信需求的时隙。网络管理器不断更新全网图路由及网络调度，以适合网络拓扑结构和通信需求的变化。图 1-3 显示了网络设备与 WirelessHART 通信协议栈之间的关系。

HART 基金会还将 HART 设备注册程序扩展到了 WirelessHART 设备。WirelessHART 设备注册流程文档概括了 WirelessHART 设备的测试和注册要求。同样的，WirelessHART 设备的注册要求确保了不同厂商提供的无线设备间的互操作性，也确保了这些无线设备能够满足 HART 通信协议规范的一致性要求。成功通过该注册要求的设备将被允许携带 HART 注册商标。

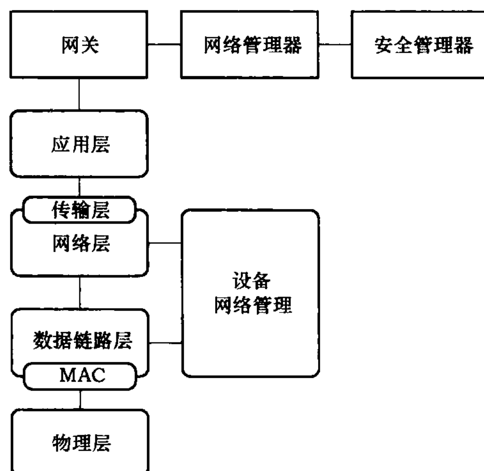



图 1-3 网络设备与 WirelessHART 通信协议栈的关系

## 1.3 协议层

图 1-4 对照 OSI 7 层协议模型描述了 WirelessHART 协议栈的体系结构。如图 1-4所示，WirelessHART 协议栈包括 5 层：物理层、数据链路层、网络层、传输层和应用层。此外，集中式网络管理器负责调度全网的路由和通信（Song 2008）。

1. 物理层

WirelessHART 物理层基本上是基于 IEEE 802.15.4-2006 2.4GHz DSSS 的物理层。该层定义了射频特征，如信号方式、信号强度和设备灵敏度。正如 IEEE 802.15.4 标准，WirelessHART 工作于 2400 ~ 2483.5MHz 的免费 ISM 频段，其数据传输速率可高达 250kbit/s。该频段被划分为 16 个信道，并被编号为 11 ~26，两个相邻信道之间的频间距为 5MHz。

2. 数据链路层

WirelessHART 标准的一个显著特征是其基于时间同步的数据链路层。WirelessHART 数据链路层的通信时隙被严格地定义为 10ms，并利用 TDMA 技术支持冲突避免和确定性通信。超帧的概念是一系列连续时隙的组合。超帧是周期性的，其周期为一组时隙的总和。WirelessHART 网络中的所有超帧都起始于 ASN 0，即网络被第一次创建的时候。然后，每个超帧按照其自身的时间周期循环重复着。在 WirelessHART 中，一个时隙的通信由这样的一个相量来描述：{frame id，index，type，src addr，dst addr，channel offset}，其中 frame id 是具体定义的超帧号，index 是超帧中时隙位置索引，type 定义时隙的类型（如发送/接收/空闲），src addr 和

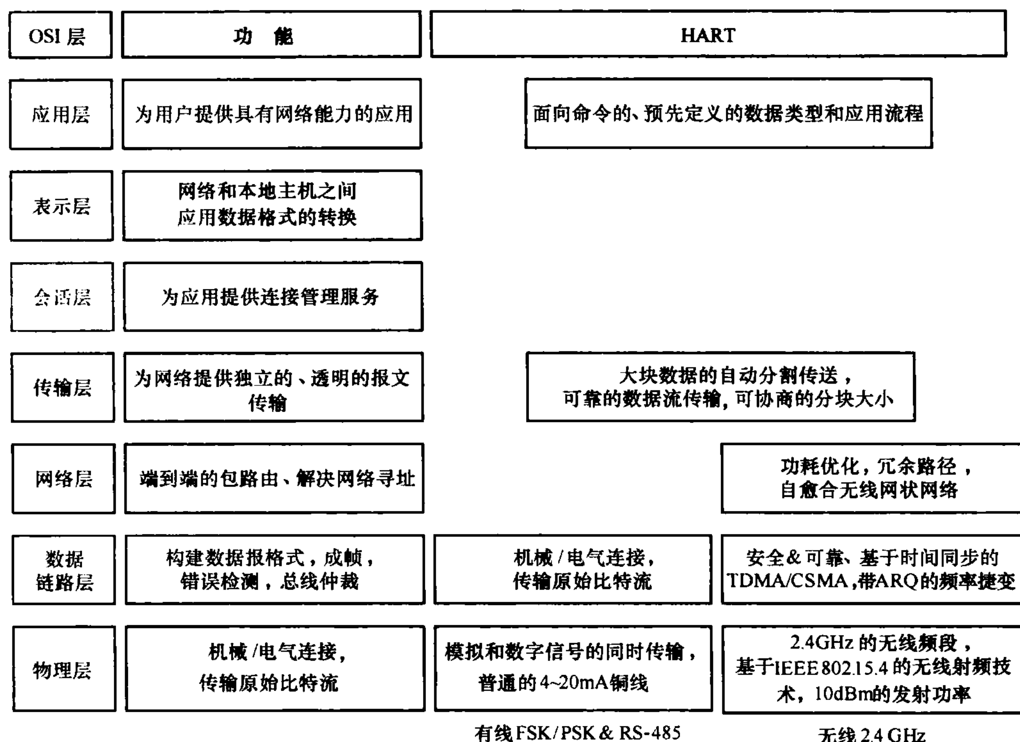



图 1-4　OSI 7 层协议模型与 WirelessHART 协议栈体系结构的对照

dst addr 分别是源设备地址和目标设备地址，channel offset 提供了用于通信的逻辑信道。为了支持跳信道功能，每个设备需要维护一个有效的信道表。由于黑名单的缘故，这个表的实际数量可能少于 16 个。对于一个给定的时隙和信道偏移量，实际的物理信道号将由以下公式确定：

$$\text{实际信道号} = (\text{信道偏移量} + \text{绝对时隙数})\ \%\ \text{可用信道数}$$

实际信道号被作为有效信道表的一个索引以得到物理信道号。因为绝对时隙数是持续不停地累加的，所以即使信道偏移量相同，不同时隙对应的物理信道也会不同。这样就可以实现信道分集，同时也可增强通信的可靠性。图 1-5 描述了数据链路层的总体设计，其中包括如下 6 个主要模块：

（1）接口　MAC 和物理层间的接口描述了物理层提供的服务原语。MAC 和网络层间的接口定义了提供给网络层的服务原语。

（2）定时器　定时器是 WirelessHART 标准中的一个基本模块，它提供精确时间以确保系统的正确操作。一个重要的挑战是如何设计定时器模块，并使那些 10ms 的时隙保持时间同步。

（3）通信表　每个网络设备维护一个数据链路层的表集合。超帧表和链路表存储了网络管理器创建的通信配置；邻居表是一个能直接通信的邻居节点列表；图路由表被用于记录路由信息，并协助网络层。

（4）链路调度器　链路调度器的功能是：基于超帧表和链路表中的通信调度信息确定下一个时隙的使用。链路调度器复杂的原因有：传输的优先级、链路的变化、超帧的使能和不使能。每个能影响链路调度的事件都将引起链路调度的重新评估。

（5）报文处理模块　报文处理模块分别缓冲来自于网络层和物理层的数据报。

（6）状态机　数据链路层的状态机由三个主要部件组成：TDMA 状态机、XMIT 和 RECV 引擎。TDMA 状态机负责执行时隙通信并调整计数器时钟。XMIT 和 RECV 引擎直接控制发送接收机的硬件部分，分别用于发送和接收数据报。

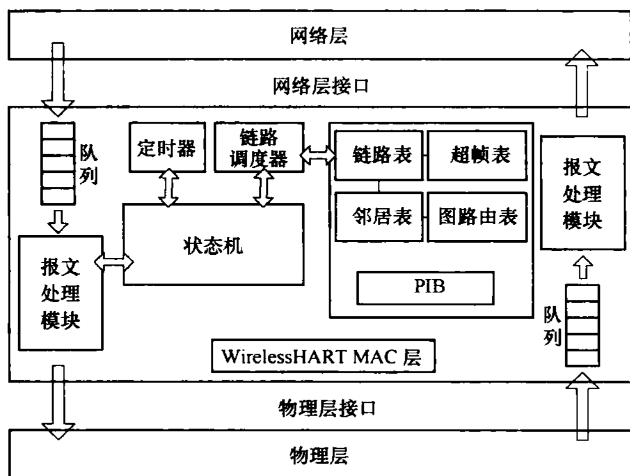



图 1-5　数据链路层的总体设计

3. 网络层和传输层

网络层和传输层共同为网络设备提供安全、可靠的通信。图 1-6 描述了网络层和传输层的整体设计。典型的 WirelessHART 网络包括以下一些基本部件：①安装于工厂工艺流程的现场设备；②手持设备：一种用于配置设备、诊断和性能校准的手持式 WirelessHART 计算机；③网关：用于连接上位机和现场设备；④网络管理器：负责配置网络，调度和管理 WirelessHART 设备间的通信。为了支持网状网络结构，每个 WirelessHART 设备都要求能为其他设备转发数据报。WirelessHART 标准定义了三种路由协议：

（1）图路由　图是一组连接网络节点的路径的集合。图中的每条路径都是被

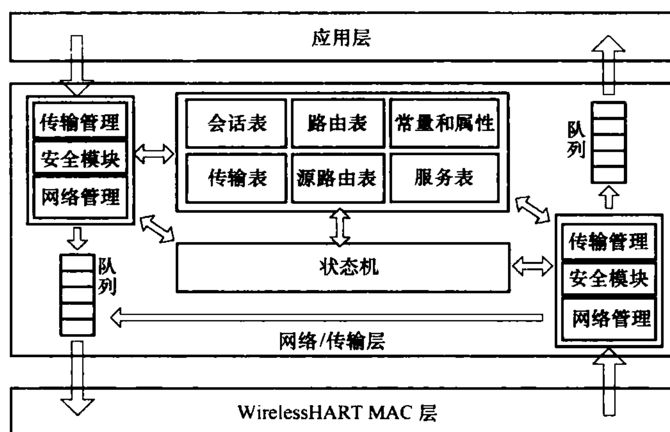



图 1-6 网络层和传输层的整体设计

网络管理器明确地创建，并被下载到每个独立的网络设备。为了发送一个数据报，源设备在数据报中的网络层头部写下一个特定的图标识符，该标识符由目标设备确定。从源节点到目标节点路径上的所有网络设备都必须被预先配置有图信息，以规定这些邻居节点如何转发数据报。

（2）源路由 作为图路由的一种补充，源路由主要用于诊断网络。为了发送一个数据报到目标设备，源设备在其数据报头部放置一个数据报传递顺序的设备列表。当数据报被传递时，每个路由设备查看列表中列出的下一个网络设备地址，从而确定出其下一跳的目标设备地址，直至数据报到达目标设备。

（3）超帧路由 超帧路由是图路由的一个特例。在超帧路由中，数据报被分配给一个超帧。数据报沿着超帧中源节点到目标节点的路由路径，从而实现数据报的路由。对于超帧路由，图标识符被设置成超帧标识符。因为数据报是沿着超帧路由的，所以不必严格配置图边界。

4. 应用层

图 1-7 描述了应用层的整体设计。应用层是 WirelessHART 标准的最顶层，它定义了各种设备命令、响应、数据类型和状态报告。在 WirelessHART 标准中，设备和网关之间的通信是基于命令和响应的。应用层负责解析报文内容、提取命令号、执行指定的命令，以及产生响应。

5. 安全体系结构

WirelessHART 网络是一种安全的网络系统。WirelessHART 的 MAC 层和网络层都提供了安全服务。MAC 层结合使用了循环冗余校验（Cyclic Redundancy Check，CRC）和消息完整性代码（Message Integrity Code，MIC），从而能提供跳到跳的数据完整性服务。尽管 CRC 的能力有限，但是它目前仍然是一种被广泛使用的技术。

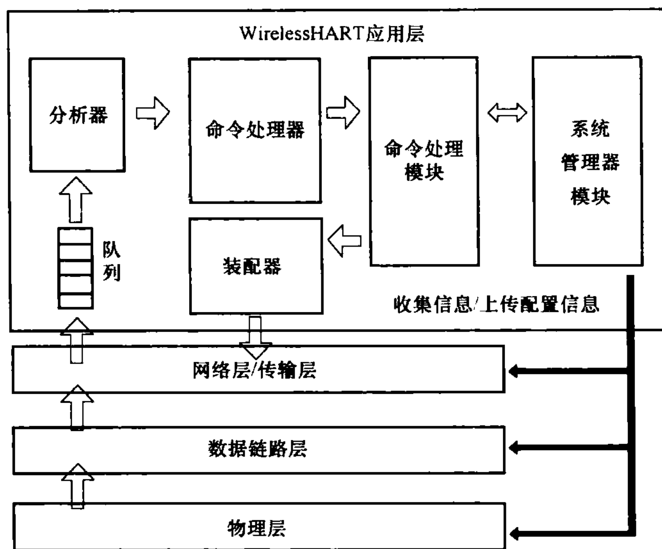



图 1-7　应用层的整体设计

发送方和接收方都使用了 CCM 模式和 AES-128 块加密算法来产生和验证 MIC。网络层采用了各种密钥以提供端到端的加密和数据完整性服务。WirelessHART 安全体系定义了四种密钥：

1）当没有网络密钥的时候，公共密钥被用来产生 MAC 层的 MIC。

2）网络密钥被所有的网络设备共享，并被网络设备用来产生 MAC 层的 MIC。

3）入网密钥对于每个网络设备而言都是唯一的。在设备加入网络过程中，入网密钥被网络管理器用来认证正申请入网的新设备。

4）会话密钥由网络管理器创建。会话密钥对于两个网络设备间的端到端连接都是唯一的，它被用来提供端到端的加密和数据完整性服务。会话密钥又可进一步分为单播密钥和广播密钥。单播密钥和广播密钥在如何存储和使用随机数（Nonce）方面是非常困难的。

图 1-8 描述了在以下两种不同的场景下如何使用这些密钥：①一个新的网络设备想加入网络；②已存在的网络设备正在与网络管理器通信。在第 1 个场景中，入网设备将需要使用公共密钥来产生 MAC 层帧头中的 MIC，还需要使用入网密钥来产生网络层 MIC 并加密入网请求报文。在入网设备被认证后，网络管理器将为该设备产生一个会话密钥，并将其通过启动包发送给该设备。这样网络管理器和该入网设备间的会话就被安全地建立了。在第 2 个场景中，在 MAC 层方面，网络密钥被用于数据链路协议数据单元（Data-Link Protocol Data Unit，DLPDU）的认证；在网络层方面，会话密钥被用于认证和加密数据报。

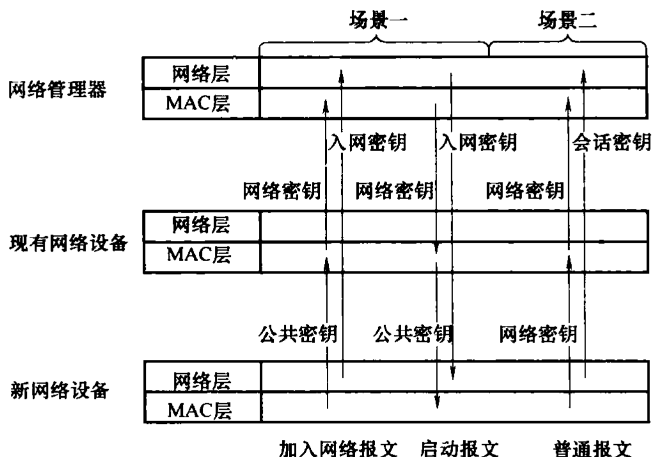



图1-8 密钥模型

## 1.4 简单案例

这里，我们将通过一个非常简单的案例来描述 WirelessHART 网络。该案例中的 WirelessHART 系统是基于 FreeScale 硬件平台实现的，其中 WirelessHART 协议栈是我们用 ANSI C 语言编写的。

该示范案例中的 WirelessHART 网络包含一个网关和两个网络设备。网关同时也扮演着接入点的角色，两个网络设备分别被定义为设备 1 和设备 2。在这个网络中，设备 1 将网关作为其时钟源，同时也作为设备 2 的时钟源。网关和设备 2 中都各自维护着一个 4 位的计数器，网关中的计数器用于累加计数而设备 2 中的计数器用于递减计数。网关和设备 2 通过设备 1 交换它们的计数器值，并通过 LED 指示灯显示各自接收到的计数器值。设备 1 的前两个 LED 指示灯用来显示网关计数器值的低 2 位，剩下的 LED 指示灯用来显示设备 2 计数器值的低 2 位。这样，我们就能通过 LED 指示灯简单地检测网关和设备 2 之间的通信状态。

我们还为该示范网络定义了一个总超帧，见表 1-1。基本上，这个超帧定义了所有通信的时序，即网关首先通过设备 1 传输数据报给设备 2，设备 2 在收到网关发出的数据报后将自己的计数器值发送给网关。

表1-1 示范案例中的超帧配置

| 时 隙 号 | 链 路 |
|---|---|
| 0 | 网关 - > 设备 1 |
| 1 | 设备 1 - > 设备 2 |
| 2 | 设备 2 - > 设备 1 |
| 3 | 设备 1 - > 网关 |

在 WirelessHART 抓包器 Wi- Analys 的帮助下，我们证实了以下情况：

1）两个设备都实现了与网络时间源（网关）的同步；

2）一个 DLPDU 总能立即在同一个时隙内被确认；

3）网关和设备 2 能通过设备 1 得到彼此的计数器值。设备 1 能为设备 2 和网关转发数据报。

因为 WirelessHART 标准工作于 IEEE 802.15.4 物理层之上和采用 IEEE 802.15.4 的 DLPDU 格式，所以我们也能通过任何硬件抓包器和 IEEE 802.15.4 协议分析仪在数据报层面上捕获 WirelessHART 网络的通信情况。

# 第2章　物　理　层

摘要：物理层定义无线设备与物理介质之间的电气和物理层关系。它定义一些特征，例如：天线、空气介质、功率等级、电压变换时间、物理数据率、最大发射功率等。WirelessHART 标准是基于 IEEE 802.15.4 标准的。WirelessHART 物理层是一个 IEEE 802.15.4 标准简化后的子集。本章列出 WirelessHART 物理层提供给其上层——数据链路层的服务。请参照 WirelessHART 物理层规范（HCF_SPEC-65）以获得更详细的信息。

WirelessHART 标准建立于 IEEE 802.15.4 之上。WirelessHART 物理层是一个针对 IEEE 802.15.4-2006 标准中物理层（如 IEEE 802.15.4－2006 标准中第 6 节所定义）简化后的子集，仅对其做了少量的修改和限制。对于任何 WirelessHART 设备：

1）每 10ms 内，都只会有一个或两个 IEEE 802.15.4 报文（广播报文不需要确认）。

2）报文间最短的时间间隔是同一时隙内的数据报文和确认报文之间的时间间隔。在一个时隙内，从数据报文结束到确认报文开始的时间间隔为 1ms。

3）所有 WirelessHART 报文都是 IEEE 802.15.4 数据类报文。

4）只采用 2.4GHz 频段。

5）信道 11～25 被允许使用。因为信道 26 在一些国家是不被允许使用的，所以 WirelessHART 不支持使用信道 26。

简而言之，WirelessHART 物理层针对发送和接收 IEEE 802.15.4 数据报文作了一些限制。以下是 WirelessHART 物理层内一些值得注意的术语：

1）跳信道：每次 WirelessHART 传输所占用的物理信道都会改变。

2）传输功率：IEEE 802.15.4 标准针对的是覆盖范围为 10m 的个人区域网络。然而，WirelessHART 网状网络能覆盖相对更大的区域。所有的设备必须提供 10dBm（10mW）±3dB 的额定等效全向辐射功率（EIRP）。发送功率可配置为－10～＋10dBm。最大室外视距传输距离能达到 100m。

WirelessHART 设备的射频硬件部分定位于使用已商业化的 IEEE 802.15.4 芯片。

## 2.1　物理层服务

本节列出物理层服务原语的操作。

### 2.1.1 信息服务原语

1. 发送接收机的使能/不使能：这个服务原语是用来使能/不使能某个信道。

1）ENABLE. request（state，channel）。

2）ENABLE. confirm（state，channel）。

3）ENABLE. indicate（）。

2. 信道空闲评估：这个服务原语促使物理层执行信道空闲评估。

1）CCA. request（）。

2）CCA. confirm（status）。

3. 数据通信服务：这些服务原语被用于物理层的数据报交换。

1）DATA. request（数据）。

2）DATA. confirm（status，data）。

3）DATA. indication（rsl，data）。

4）ERROR. indication（status，data）。

### 2.1.2 管理服务原语

这个服务原语被用来配置物理层。

1）LOCAL_MANAGEMENT. request（service，[data]）。

2）LOCAL_MANAGEMENT. confirm（service，status，[data]）。

3）LOCAL_MANAGEMENT. request（service，status，[data]）。

管理服务原语中的第一个参数是请求的服务类型。表 2-1 列出了服务类型。

表 2-1 本地设备管理命令

| 服务 | 数据 | 描述 |
|---|---|---|
| RESET | — | 初始化物理层 |
| READ_TX_PWR_LEVEL | 8 位有符号型的 txPwrLevel | 读取发送功率（dBm） |
| WRITE_TX_PWR_LEVEL | 8 位有符号型的 txPwrLevel | 写入发送功率（dBm） |
| WRITE_SLEEP_STATE | 8 位无符号型的 slepState | 写物理层睡眠状态，取值于｛睡眠，苏醒｝ |
| WRITE _ RCV _ OVERFLOW _ENABLE | 布尔型的 rcvOverflowEnable | 使能接收机溢出错误指示。这个将被报告于 ERROR. indication（）服务状态中 |

# 第3章 数据链路层

摘要：数据链路层检测和校正物理层中可能发生的错误，从而为网络节点之间提供可靠的数据传输。数据链路层的主要任务是创建和管理数据帧，其通常被细分为两个子层：逻辑链路控制（Logical Link Control，LLC）子层和介质访问控制（Medium Access Control，MAC）子层。逻辑链路控制子层为网络层定义服务，而介质访问控制子层定义多个节点如何分享通信介质。本章将列出WirelessHART数据链路层给网络层提供的服务，也将进一步更详细地描述逻辑链路控制子层和介质访问控制子层。同时，我们将描述报文格式、WirelessHART的流控制、错误检测和安全。我们还将描述如何维护基于TDMA的时隙同步，如何为侦听邻居节点的数据报而调度时隙，以及如何发送来自于网络层的数据报等。请参阅TDMA数据链路层规范（HCF_SPEC-75）以获取更详细的信息。图3-1显示了数据链路层的范围。

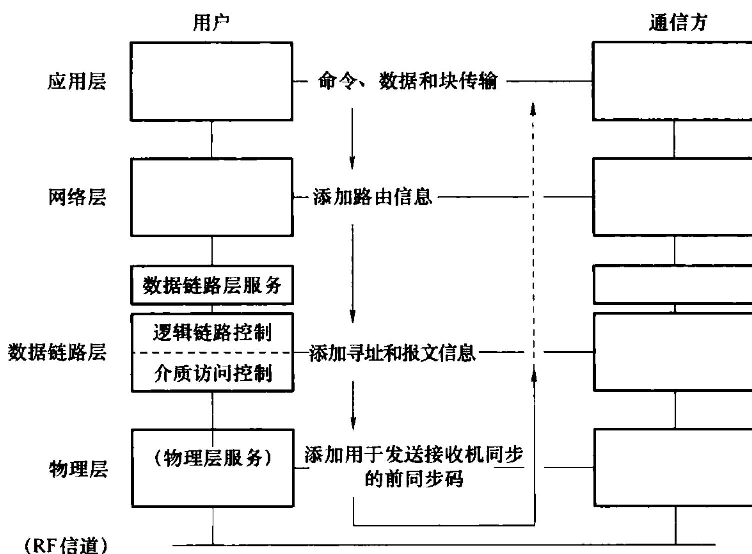



图3-1 数据链路层的范围

数据链路层规范包括：

1）数据链路层为网络层提供的服务。这些服务构成了一个数据链路层要求的黑盒模型。

2）逻辑链路控制子层的要求包括：HART 帧格式、HART 设备地址结构、用于信息完整性的安全服务和错误检测代码。

3）介质访问控制子层定义的规则确保了众多设备都能有序地发送数据。换句话说，介质访问控制子层规定了设备什么时候被允许发送一个数据。

4）满足介质访问控制子层正确操作的实际时间值。这些实际时间值直接反映了一些物理层性能特征（如信道评估时间、发送/接收状态转换时间）。

## 3.1 数据链路层服务

### 3.1.1 报文服务原语

报文服务原语提供了支持设备间基本数据传输的服务。数据链路层也必须允许报文队列。协议也支持自动重传以确保准确的数据交换。

1. 发送服务原语

1）FLUSH. request （handle）。

2）FLUSH. confirm （handle，localStatus）。

3）TRANSMIT. confirm （handle，localStatus）。

4）TRANSMIT. indicate （localStatus，priority，sourceAddress，payload）。

5）TRANSMIT. request （handle，payload，priority，timeout，graph）。

6）TRANSMIT. request （handle，payload，priority，timeout，sframe，bcast）。

7）TRANSMIT. request （handle，payload，priority，timeout，shortDestAddress）。

8）TRANSMIT. request （handle，payload，priority，timeout，longDestAddress）。

TRANSMIT. request 服务原语的载荷参数包括：

1）handle—被用于为客户层提供便利的服务。数据链路层在其对应的 TRANSMIT. confirm 服务原语中返回这个值。

2）payload—将要被传播给目标设备的网络层协议数据单元（NL-Protocol-Data-Unit，NPDU）。

3）priority—数据报优先级，其取决于载荷（payload）的内容，其取值集合为{管理，进程数据，普通，报警}。

4）timeout—允许数据报发送的最大时间。网络层应该基于 ASN Snippet 来设置这个参数（请见 WirelessHART 网络管理规范）。

5）graph—这个参数仅用于图路由模式。当使用图路由模式时，参数 graph 指明了可能被用作下一跳目标节点的邻居节点。

6）sframe—这个参数仅用于当广播某个报文的时候。参数 sframe 告诉超帧谁的广播链路能用于转发数据报。

7) bcast—这个标志位表明 NPDU 必须在指定的超帧中广播。
8) shortDestAddress—这个参数指明了下一跳目标节点的昵称。
9) longDestAddress—这个参数指明了下一跳目标节点的唯一标识符。
2. 网络事件服务原语
1) DISCONNECT. indicate (localStatus, sourceAddress)。
2) PATH_FAILURE. indicate (localStatus, sourceAddress)。
3) ADVERTISE. indicate (localStatus, AdvertisePayload)。
4) NEIGHBOR. indicate (localStatus, sourceAddress, packetRSL)。
3. 接收服务原语
1) RECEIVE. indicate (localStatus, packetRSL, payloadDLPDU)。

### 3.1.2 管理服务原语

管理服务原语既可用于配置数据链路层，也可用于访问数据链路层的统计信息。

1) LOCAL_MANAGEMENT. request (service, [data])。
2) LOCAL_MANAGEMENT. confirm (service, status, [data])。
3) LOCAL_MANAGEMENT. indication (service, status, [data])。

第一个参数 service 表明被请求的服务类型。表 3-1 列出了这些服务类型。

表 3-1　当地设备管理命令

| 服　务 | 描　述 |
|---|---|
| RESET | 初始化数据链路层 |
| DISCONNECT | 从网络中断开，中止通信 |
| RE_JOIN | 从网络中断开，重新入网，清除所有的 MAC 层报文队列和清除所有的 MAC 层列表 |
| WRITE_SUPERFRAME | 创建一个新超帧 |
| DELETE_SUPERFRAME | 删除一个已有的调度超帧和相关的链路 |
| ADD_LINK | 给另一个设备添加一个新链路，在该过程中可能会更新邻居设备列表和链接列表 |
| DELETE_LINK | 删除一个已有的链路，在该过程中可能会更新邻居设备列表和链接列表 |
| ADD_EDGE | 给某个特定图添加一个新邻居设备 |
| DELETE_EDGE | 从某个特定图中删除一个邻居设备 |

（续）

| 服　务 | 描　述 |
|---|---|
| READ_NETWORKID | 读取设备所属网络的网络 ID |
| WRITE_NETWORKID | 写入设备所属网络的网络 ID |
| WRITE_NETWORK_KEY | 该命令允许网络管理器向某个网络设备写入网络密钥。应该防止网络密钥被偷窃（例如可以通过加密来防范） |
| READ_TIMEOUT _PERIODS | 读取时间周期值，Keep-Alive、Path-Failure、Advertise 和 Discovery |
| WRITE_TIMEOUT_PERIOD | 写入某个指定的时间周期值 |
| READ_CAPACITIES | 读取 maxSuperframes、maxLinks、maxNeighbors 和 maxPk-tBuffers |
| READ_PRIORITY_THRESHOLD | 读取可接受来自于其他设备的最低优先级 DLPDU |
| WRITE_PRIORITY_THRESHOLD | 写入可接受来自于其他设备的最低优先级 DLPDU |
| READ_JOIN_PRIORITY | 读取设备应该广播的加入优先级 |
| WRITE_JOIN_PRIORITY | 写入设备应该广播的加入优先级 |
| READ_PROMISCUOUS_MODE | 读取子层是否处于“全接收”模式 |
| WRITE_PROMISCUOUS_MODE | 写入子层是否处于“全接收”模式 |
| READ_MAX_BACK_OFF_EXPONENT | 读取用于共享时隙中的退避指数的最大值 |
| WRITE_MAX_BACK_OFF_EXPONENT | 写入用于共享时隙中的退避指数的最大值 |

## 3.2 逻辑链路控制

### 3.2.1 DLPDU

每个数据链路层数据报（DLPDU）都包含以下一些字段（见图3-2）：

1）定值为 0x41 的单字节；

2）1 个字节的地址说明符；

3）1 个字节的序列号；

4）2 个字节的网络号；

5）2 个字节或 8 个字节长的目标地址和源地址；

6）1 个字节的 DLPDU 说明符；

7）数据链路层载荷；

8）4 个字节的消息完整性代码（MIC）;

9）2 个字节的 ITU-T CRC16。

图 3-2 描述了 PhPDU 和 DLPDU 基本结构。

1. DLPDU 分类符

DLPDU 分类符的定义如图 3-3 所示。它规定了优先级、报文类型、是否使用网络密钥或公共密钥认证报文。

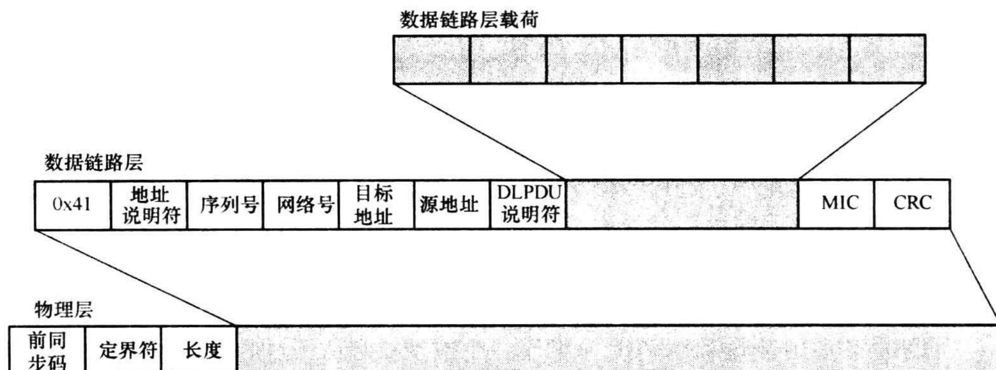



图 3-2　DLPDU 结构

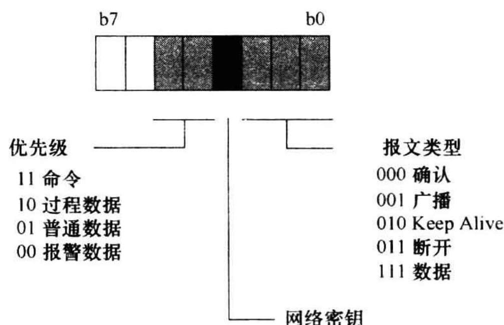



图 3-3　DLPDU 分类符的定义

2. 加密的消息完整性代码

加密的消息完整性代码（Message Integrity Code，MIC）用于数据链路层的 DLPDU 认证。设备仅响应通过认证的单播和非确认 DLPDU。

## 3.2.2　DLPDU 类型

DLPDU 分类符定义了 5 种类型的 DLPDU，如下所示：

1）Data DLPDU：包含有传送给目标设备的网络数据和设备数据；

2）Keep-Alive DLPDU：促进维护相邻设备间的连接；
3）Advertise DLPDU：为相邻的入网设备提供信息；
4）Disconnect DLPDU：用于向邻居设备广播“某设备正在离开网络”；
5）ACK DLPDU：用于在数据链路层立即回复源设备发送的 DLPDU。

### 3.2.3　DLPDU 优先级和流控制

DLPDU 分类符定义了 4 种优先级。具有最高命令优先级的网络管理数据报总是优先被传送，以便网络管理器维护网络的运作。为了防止警报洪泛破坏网络的运行，警报报文在网络中的流动被进行了严格的限制。由于报警总是以时间标记，所以相关信息（如故障时序）不会丢失。

最后，当缓冲空间和网络带宽允许时，所有其他网络数据都可以在网络中流通。在这些网络流量中，过程数据享有一定的优先级。过程操作和控制的优先级仅次于防止网络通信中断操作的优先级。

### 3.2.4　错误检测代码和安全

加密的 MIC 用于确保 DLPDU 来源于一个被授权和认证过的设备。DLPDU 本身是不加密的，但是它的内容是通过 MIC 来认证的。MIC 是使用 IEEE 802.15.4 标准中描述的 CCM 算法计算出的。这也使得现成商用芯片中的 CCM 硬件加速器可以被直接使用。

Well-known 密钥和网络密钥是数据链路层的两种密钥。Well-known 密钥用于广播和新设备入网的时候，而网络密钥用于所有其他的数据交换。所有 WirelessHART 设备的 Well-known 密钥都是相同的，其 16 进制值为 7777 772E 6861 7274 636F 6D6D 2E6F 7267。Well-known 密钥被用于欲入网设备和已入网设备间的信息交互。Well-known 公共密钥是“www.hartcomm.org”16 位字符串对应的 ASCII 值序列。

## 3.3　介质访问控制

介质访问控制子层的主要目标是维护时隙同步、识别出必须被服务的时隙、侦听来自于邻居设备的数据报、相应地将网络层传送来的数据报转发出去。

### 3.3.1　时隙

时隙内的所有操作都需要满足规定的时间要求。图 3-4 所示为一个通信时隙，同时也概述了时隙内通信的事务时序。时序符号见表 3-2。

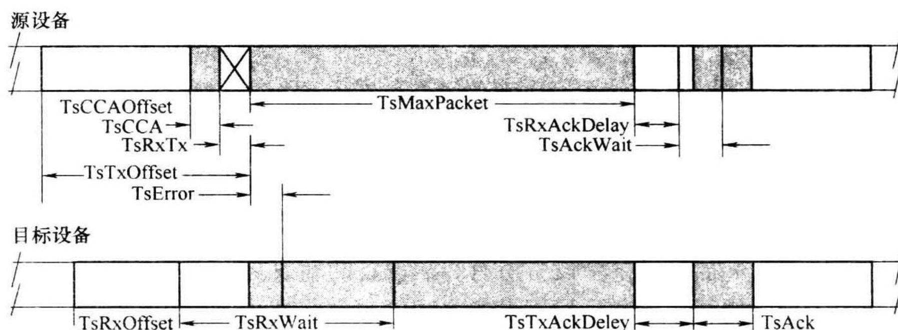



图 3-4　通信时隙

**表 3-2　时隙内通信的时序符号**

| 符　号 | 描　述 |
|---|---|
| TsTxOffset | 从时隙开始到开始传送报文中前同步码之间的时间间隔 |
| TsRxOffset | 从时隙开始到接收方必须开始侦听报文之间的时间间隔 |
| TsRxWait | 等待报文开始的最短时间。该最短时间与邻居设备间在维持通信的前提下能容忍的偏移量有关 |
| TsError | 报文的实际开始时间与接收方期望的报文开始时间之间的误差。换句话说，该值也可被认为是接收方与发送方之间的时间同步误差 |
| TsMaxPacket | 最长报文（包括物理层前同步码、定界符、长度和 DLPDU）所需的发送时间 |
| TsTxAckDelay | 从数据报文的发送结束到确认报文开始之间的时间间隔。接收方必须确认数据传输的开始，并且在此期间产生一个确认报文<br>注意：广播报文不需要确认 |
| TsRxAckDelay | 从数据报文的发送结束到发送方必须开始侦听确认报文之间的时间间隔 |
| TsAckWait | 等待确认报文开始的最短时间 |
| TsAck | 确认报文所占用的发送时间 |
| TsCCAOffset | 从时隙开始到 CCA 开始的时间间隔 |
| TsCCA | CCA 的执行时间 |
| TsRxTx | 发送状态与接收状态之间的切换时间 |

## 3.3.2　通信表和缓冲区

所有设备都维护着一系列通信表。这些通信表用于控制所有设备的通信和收集这些通信的统计信息。此外，数据报在接收、处理和转发的过程中可能需要被缓冲

起来。

控制通信行为的表包括：

1）超帧表：网络管理器可能配置多个超帧。

2）链路表：与某设备相关的所有链路的列表。超帧中的每个链路都被配置成用来与某个特定邻居设备通信，或者广播给所有在这个链路中处于侦听状态的设备。

3）邻居表：邻居表是某个设备所有邻居设备的列表。

4）图表：图用于源设备到目标设备之间的数据报路由。设备并不知道整个路由路径。然而，图指明了下一跳目标设备，这样数据报就可被依次传递至最终目标设备。

### 3.3.3 链路调度

所有设备都必须维护一个链路调度以识别下一个时隙所对应的服务。时隙所对应的服务既包括侦听一个新数据报，又包括通过网状网络转发一个数据报。当一个时隙同时要被用于发送一个数据报和接收一个数据报的时候，发送数据报比接收数据报的优先级高。

链路调度表面上看起来简单。然而，由于事务优先级、链路变换、超帧的使能或不使能等诸多原因，链路调度实际上很复杂。每个影响链路调度的事件都可能会引起大范围的链路重新分配。例如，如果一个高优先级事务的发送失败了，那么它必须被重新调度分配。这样，低优先级的事务可能会被延缓至后一个链路，从而将当前的链路让给该优先级更高的事务。这样的影响可能会是更大范围的，例如一个超帧被不使能了或被删除了。

# 第 4 章　网络层和传输层

摘要：在ISO™OSI™七层协议模型中，网络层负责网络路由功能，主要处理网络寻址和数据传输。传输层通过流控制、分段和合并、错误控制等机制来控制两个网络节点之间的可靠的、及时的传输。会话层负责在两个网络节点之间建立、维持和终止通信会话。在 WirelessHART 标准中，网络层包含了所有上述三层的功能。同时，它还是传统 HART 令牌传送网络和 WirelessHART 基于时分复用网络的交汇处。本章列举了网络层为其上层——应用层提供的各种服务，并描述了网络层的通信、路由和安全问题以及网络层数据报的格式。更多的细节请参考 WirelessHART 网络管理规范（HCF_SPEC-85）。

## 4.1　概述

图 4-1 描述了网络层的范围，这也是本章的重点。WirelessHART 标准中的网络层包含了一层很薄的传输层，并且还拥有会话层的功能。HART 应用层位于网络层之上，它定义了 HART 允许的数据类型、程序和各种命令。在网络层之下是两个主要的 HART 规范：有线令牌传送网络和基于时分复用的无线通信技术。本章主要涉及其中的无线部分。

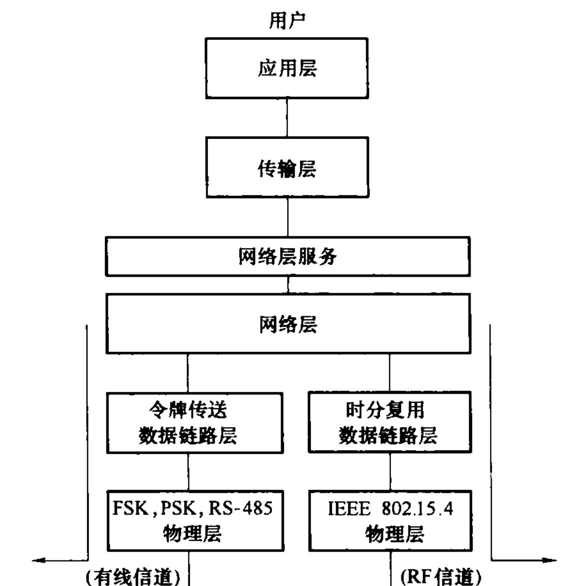



图 4-1　网络层的范围

### 4.1.1　通信量

HART 支持多种类型的网络通信服务，其中包括：

1）请求/响应。这是上位机与某个指定设备之间的直接通信。在这种通信中，源设备地址和目标设备地址是明确给定的。请求和响应的内容由具体的 HART 命令给出。

2）过程数据的发布。某些 HART 命令被用来请求过程数

据，然后以命令响应的方式被发布。

3）广播报文使用标准的 HART 请求/响应类型，但是其目标地址使用的是广播地址。

4）块数据传送在两个网络节点之间建立一个管道来支持数据在它们之间以流的形式进行传输。

图 4-2 给出了 WirelessHART 数据报的格式。

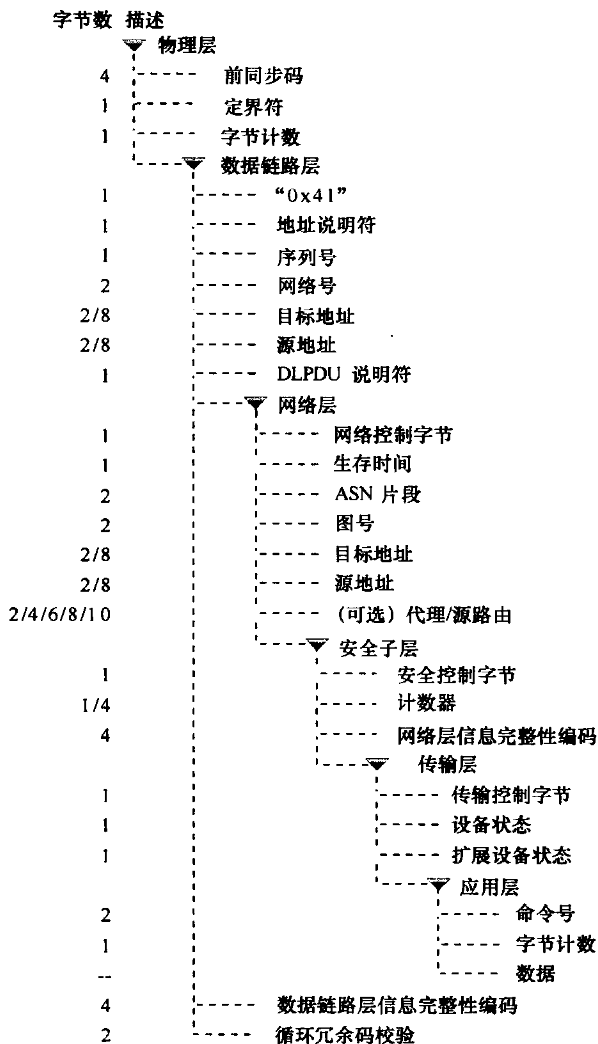



图 4-2 WirelessHART 数据报格式

### 4.1.2　路由

WirelessHART 网络层支持两种路由方式：图路由和源路由。

1）图：一个图路径是网络拓扑的一个子图。它为源设备和目标设备之间提供了带有冗余路径的通信路径。当数据报从源设备传输到目标设备的时候，实际的通信路径根据当前的网络状况来决定。

2）源：源路径是建立在源设备和目标设备之间的一条有向路径。源路径在数据报的网络层头部中被静态地指明了。

### 4.1.3　安全

网络层通过建立会话来管理端对端的通信。一个设备对于它的对端设备可以定义多于一个的会话。对于每个它参与的会话，该设备都必须维护对应的安全信息（加密密钥，随机数计数器）和传输层信息（可靠传输序列号，重传计数器等）。网络中的任意两个设备都可以建立会话。

## 4.2　网络层服务

### 4.2.1　网络层报文服务原语

消息服务原语提供各种服务来支持设备之间的基本数据传输。网络层支持请求/响应通信和单向通知。

1）TRANSMIT. request（handle，dest，priority，timetableID，transportType，payload）。

2）TRANSMIT. indicate（handle，srcAddr，priority，transportType，payload）。

3）TRANSMIT. response（handle，payload）。

4）TRANSMIT. confirm（handle，localStatus，[payload]）。

5）FLUSH. request（handle）。

6）FLUSH. confirm（handle，localStatus）。

TRANSMIT. request 服务原语包括以下参数：

（1）handle　网络层在对应的 TRANSMIT. confirm 服务原语中返回这个值使得应用层可以对请求和响应进行匹配。

（2）Dest　数据报的目标地址。

1）UniqueID：目标设备的长地址。

2）Nickname：目标设备的短地址。

3）Broadcast：广播地址。广播地址在网络层头部中被标明。网络层头部中的

控制字节标明其是一个短的目标地址。

(3) Priority　数据报的优先级，其由有效载荷的内容决定。它可以是 {管理，进程数据，普通，报警} 中的一个。更多关于数据报优先级的内容请参考“TDMA 数据链路层技术规范”。

(4) TimetableID　时间表号。通信的发起者需要负责在通信开始前从网络管理器中获得足够的通信带宽。时间表号标识了这次通信请求的带宽。如果网络中剩余的带宽不足以完成此次请求，那么这个服务原语就会返回一个错误提示，同时有效载荷也不会被传输。

(5) transportType　传输类型（见表 4-1）标识了传输层请求的操作。传输类型用来设置网络头部中的传输字节。

(6) Payload　有效载荷，即要被传输到目标地址的内容。

**表 4-1　传输类型编码**

| 编码 | 描　述 | 是否广播 | 是否应答 | |
|---|---|---|---|---|
| 0 | 传输请求。主要用于块数据传输机制（主动端） | — | — | →请求 |
| 1 | 传输响应。主要用于块数据传输机制（从动端） | — | — | ←响应 |
| 2 | 单播请求（仅用于 TRANSMIT. request）。用于主动端设备执行请求/响应通信（例如，配置设备） | — | X | →请求 |
| 3 | 单播响应（仅用于 TRANSMIT. response）。用于从动端设备执行请求/响应通信（例如，配置设备） | — | X | ←响应 |
| 4 | 搜索广播（仅用于 TRANSMIT. request）。用于发送一个广播数据报以发现一个具体的设备（例如，命令 21） | X | — | →请求 |
| 5 | 发布广播（仅用于 TRANSMIT. response）。用于发送一个广播数据报给所有的网络设备（例如，时间广播） | X | — | ←响应 |
| 6 | 请求广播（仅用于 TRANSMIT. request）。（例如，改变网络号） | X | X | →请求 |
| 7 | 响应广播（仅用于 TRANSMIT. response）。这是对应于请求广播的单播响应 | X | X | ←响应 |
| 8 | 发布/通知（仅用于 TRANSMIT. response）。（例如，过程数据） | — | — | ←响应 |

除了当前正在处理的数据报以外，网络层还必须能够缓存至少一个额外的数据报。

## 4.2.2　网络层管理服务

网络层管理服务原语既可用来配置网络层，又可用来访问网络层收集到的统计信息。网络层管理服务原语的格式如下：

1) LOCAL_MANAGEMENT. request（service，[data]）。

2) LOCAL_MANAGEMENT. confirm（service，status，[data]）。

3）LOCAL_MANAGEMENT. indication（service，status，[data]）。

网络层管理服务原语中的第一个参数是被请求的服务类型。表 4-2 汇总了这些服务类型。

表 4-2　本地设备管理命令

| 服务类型 | 描述 |
|---|---|
| RESET | 重置和初始化网络层。当调用这个原语的时候，所有的网络表都会被清空。通常，该服务原语在设备通电或者当设备被安装到一个新的网络中的时候被调用 |
| WRITE_SESSION_KEY | 设置会话和随机数（nonce） |
| DEL_SESSION | 删除一个会话 |
| ADD_ROUTE | 为某个给定的目标地址增加一条路由路径 |
| DEL_ROUTE | 删除路由信息 |
| DEFAULT_ROUTE | 将指定的路由设置为默认路由 |
| READ_PDU_TIMEOUT | 读取数据报的超时值。数据报的超时值是指该数据报从产生到被丢弃的时间。设备比较 ASN 片段和当前 ASN 的值来决定数据报是否超时，从而决定是否丢弃该数据报 |
| WRITE_PDU_TIMEOUT | 写入数据报的超时值 |
| READ_TTL | 读取数据报的生存时间值。数据报的生存时间值在该数据报产生的时候被初始化 |
| WRITE_TTL | 写入数据报的生存时间值 |

## 4.3　网络层规范

网络层提供了路由、端对端安全，以及传输的功能。它管理着一对设备之间的端对端会话。

### 4.3.1　网络层 PDU

如图 4-3 所示，WirelessHART 网络层 PDU（Network Layer Protocol Data Unit，NPDU）包括三个不同的部分。首先，网络层包含了一些字段，这些字段用于将 NPDU 路由至目的地。其次，在网络层之上是一个安全层，用于保证这个 NPDU 的端对端通信不受干扰。最后一个部分是 NPDU 的有效载荷，它包含了在网络上将被交换的有效数据信息并被加密。以上三个部分合起来组构成了一个 NPDU。

#### 4.3.1.1　网络层

NPDU 部分包括以下几个字段：

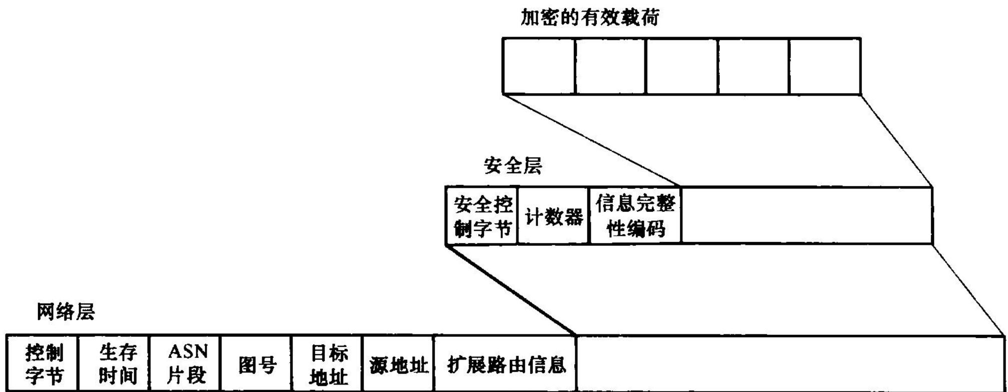



图 4-3 WirelessHART NPDU 结构

1）1 个字节的控制字段；
2）1 个字节的生存时间计数器（以跳为单位）；
3）ASN 中的 2 个最低有效字节（延迟计数器）；
4）2 个字节的图号；
5）目标地址和源地址；
6）可选的路由字段。

除了包含以上这些字段，完整的 NPDU 还包括安全字段以及后面被加密的有效载荷。

（1）控制字节 NPDU 的第 1 个字节是控制字节（参见图 4-4）。这个字节的前 2 位（第 7 位和第 6 位）说明了源地址和目标地址是 8 字节的长地址（EUI-64™地址）还是 2 个字节的短地址。后面的 3 个位（位 5 ~ 位 3）为保留位。位 2 ~ 位 0 用于表明数据报中是否存在路由字段。如果位 2 ~ 位 0 被置 1，那么三个路由字段都将会被使用，代理路由是 2 个字节长度，每个源路由是 8 个字节长度。所以，网络层的长度可以根据位 2 ~ 位 0 的值而被扩展成 2、10 或者 18 个字节。当 WirelessHART 设备中的网络层接收到一个 NPDU 时，它将检查该 NPDU 中的目标地址；如果该目标地址与自己的设备地址相一致，那么该设备将校验该 NPDU，并且解密 NPDU 中的载荷。一旦校验和解密成功，带有该载荷的 transmit. indicate 原语将被调用。

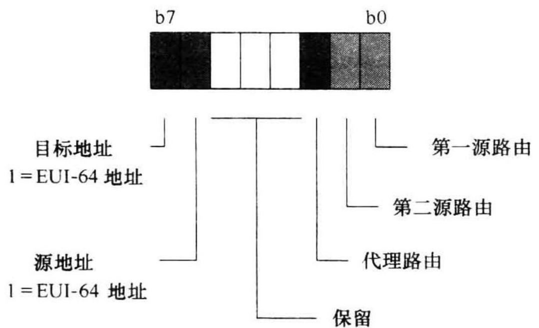



图 4-4 网络控制字节

（2）生存时间　每当设备接收到一个数据报后，设备将数据报中的目标地址与自己的地址相比较。如果地址不匹配，那么设备的网络层将依据数据报中的生存时间计数器值来决定是转发还是丢弃此数据报。生存时间计数器的值决定了数据报的生存时间。数据报每被转发一次，生存计数器将减 1。当生存时间计数器的值等于 0 时，此数据报将不会被转发到其他设备。当网络层接收到数据，如果数据报中生存时间计数器的值为 0xFF，那么该生存时间计数器的值将不会被减 1，而会被一直转发至目标地址，即该数据报的生存时间是无限的。

（3）ASN 片段　当网络层的 TRANSMIT. request 服务原语被调用时，当前 ASN 计数器中最低有效 16 位将会被放置于该 ASN 片段。这个字段提供了粗糙但是关键的实时性能指标和网络运行的诊断信息。当完整的 ASN 被再现的时候，它也可以用于计算数据报的寿命。

如果数据报中的生存时间是有效的，那么设备的网络层将数据报产生时的 ASN 值和当前 ASN 值相比较，从而可以得出该数据报的寿命。如果该数据报的寿命大于 maxPacketAge，那么该数据报将会被丢弃掉；如果该数据报的寿命小于 maxPacketAge，那么该数据报以及该数据报的寿命将会被传送给数据链路层。

（4）图号　图号被用来路由一个数据报到它的目标地址。图号用于识别一组节点。这组节点中的任何一个都可以被用来转发这个数据报到它的目标地址。否则的话，我们将根据网络层头部中存在的其他路由信息来转发数据报。

（5）源地址/目标地址　源地址和目标地址的长度可以是 2 个字节或者 8 个字节。更多的信息请参考 WirelessHART 标准中"TDMA 数据链路层规范"。源地址和目标地址在 NPDU 转发的过程中不会被改变。

#### 4.3.1.2　安全子层

NPDU 的安全层头部被设计用来保证两个设备之间的通信不受干扰，并可用于将来进一步增强 WirelessHART 的安全性能。

如图 4-5 所示，安全控制字节包含了 4 个枚举型的数据位（位 0 ~ 位 3），用来标识该 NPDU 所采用的安全策略（参见"规范 HCF_SPEC-183"中的通用表 53）。安全控制字节中的高 4 位是保留位。

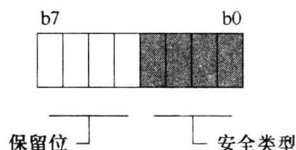


图 4-5　安全控制字节

此外，在安全层头部中，计数器字段的值被作为随机数（nonce）计数器用于加密算法的运算。

#### 4.3.1.3　有效载荷

为了安全起见，当 NPDU 在网络上传输的时候，其有效载荷字段一直被加密以保证不被中间节点获得其内容信息。NPDU 的有效载荷由传输层信息、事务 ID、设备状态、扩展设备状态以及一个或者多个命令组成。

### 4.3.2 传输层 PDU

传输层保证数据报可以经过多跳通信传送到最终的目标设备。传输层支持基于确认和非确认的通信。每个传输层 PDU（Transport Layer Protocol Data Unit，TPDU）都包含以下一些字段：

1）一个传输字节来保证端对端的数据传输；

2）设备状态和扩展设备状态字节；

3）一个或者多个 HART 命令。

图 4-6 展示了基本的 TPDU 的结构。传输层的通信可以被用于：

1）一个主控设备发出一个请求数据报，一个或者多个从控设备发出响应数据报以应答；

2）一个从控设备发布一个响应数据报。

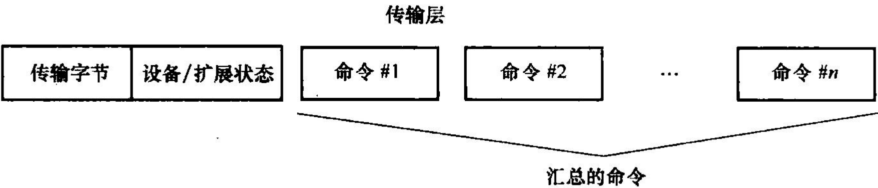



图 4-6 TPDU 结构

（1）传输字节 TPDU 的第一个字节是传输字节（见图 4-7）。

（2）设备/扩展状态 所有的 TPDU 都包含设备状态和扩展设备状态。它们的格式可以参阅 WirelessHART 标准中的“命令汇总规范”。

（3）命令汇总 在满足一些限制条件下，WirelessHART 标准允许一次通信可以同时传输多个 HART 命令。图 4-8 描绘了在 WirelessHART 网络上被传输的命令格式。

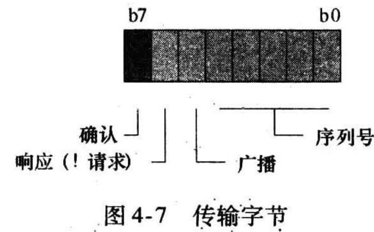



图 4-7 传输字节




图 4-8 WirelessHART 命令格式

# 第5章 应 用 层

摘要：在OSI协议层次模型中，应用层是最接近终端用户的一层，它为用户提供访问网络信息的接口。应用层的主要功能通常包括识别通信对象、确定资源可利用性和同步通信。在WirelessHART应用层，命令是通信的积木。本章将罗列出WirelessHART应用层提供给上位机的应用服务、描述动态和设备变量，以及上位机一致性分类。

WirelessHART标准中的“命令汇总规范（HCF_SPEC-99）”定义了基本的应用层，如下：

1）允许通过协议发送的数据格式；

2）所有现场设备的修订规则；

3）针对通用命令、常规命令、设备特定命令和设备族命令的编号分配；

4）构建任何HART命令的要求；

5）对所有命令响应都要求返还的命令状态字节；

6）动态变量和现场设备变量的使用；

7）主设备识别现场设备和管理HART网络的程序；

这些要求提供了所有HART应用层规范的基础。

## 5.1 应用层接口

应用层是基于命令的。换句话说，主设备和从设备发出的命令是HART通信的基础，命令号决定了命令的内容。命令号对应着一个带有一个固定字节数的、唯一的、明确的数据报格式。

1. 命令号的划分

命令可被划分为以下几类（见表5-1）：

（1）通用命令　被所有HART设备都支持的命令集合；

（2）常规命令　适用于大部分设备的命令集合，设备应该尽可能地支持该种命令；

（3）非公共命令　一类特别的命令集合，这些命令仅在制造现场设备的过程中使用。这些命令不应该在使用现场设备的时候被调用；

（4）无线命令　支持WirelessHART产品的命令集合；所有支持WirelessHART标准的产品必须实现所有的无线命令；

（5）设备族命令　某种类型现场设备所共有的、并可以被用来设置设备参数的通用命令集合。用户仅使用设备族命令就可以调用该类设备，而无需使用设备特定命令或设备特有的驱动软件。

（6）设备特定命令　设备制造商根据现场设备的需要而定义的命令。

**表 5-1　HART 命令号的划分**

| 命令号 | 命令类型 | 描述 |
| --- | --- | --- |
| 0~30，38，48 | 通用命令 | 参见通用命令规范 |
| 31 | 扩展标志命令 | 用于标识命令的数据字段中有一个 16 位的命令存在。参见网络管理器规范 |
| 21~121（除 38 和 48） | 常规命令 | 参见常规命令规范 |
| 122~126 | 非公共命令 | 仅在现场设备制造的过程中，被工厂使用 |
| 127 | 保留 | — |
| 128~253 | 设备特定命令 | 参见制造商的设备规范文档 |
| 254~511 | 保留 | — |
| 512~767 | 额外的常规命令 | 参见常规命令规范 |
| 768~1023 | WirelessHART 命令 | 参见无线命令规范 |
| 1024~33791 | 设备族命令 | 参见设备族命令规范 |
| 33792~64511 | 保留 | — |
| 64512~64763 | 无线设备特定命令 | 这些命令号码被保留给无线网络制造商规定的命令 |
| 64766~64767 | 保留 | — |
| 64768~65021 | 额外的设备特定命令 | 仅当 128~253 命令号被设备消耗殆尽时，这些命令才会被使用 |
| 65022~65535 | 保留 | — |

表 5-2 描述了标号范围为 768~1023 的 WirelessHART 命令。这些命令被用于支持网络管理和网关功能。

2. 命令需求

1）HART 命令必须被设计为自发的，从而允许设备应用层的无状态操作。

2）一个 HART 命令必须仅实现以下功能中的某个功能：读、写或命令。

3）命令可能包含允许访问存储在现场设备中的数据组或数据表的索引。

4）多事务命令应该仅在某个设备用尽允许的一系列设备特定命令时才被使用到。

表 5-2　WirelessHART 命令

| 分　类 | 命令号 | 描　述 |
| --- | --- | --- |
| 预配置 | 768 | 写入入网密钥 |
| | 769 | 读取入网状态 |
| | 770 | 请求主动通告 |
| | 771 | 强制进入入网模式 |
| | 772 | 读取入网模式的配置信息 |
| | 773 | 写入网络号 |
| | 774 | 读取网络号 |
| | 775 | 写入网络标签 |
| | 776 | 读取网络标签 |
| | 797 | 写入射频输出功率 |
| | 798 | 读取射频输出功率 |
| | 781 | 读取设备昵称地址 |
| | 962 | 写入设备昵称地址 |
| 管理超帧和链路 | 783 | 读取超帧列表 |
| | 965 | 写入超帧 |
| | 966 | 删除超帧 |
| | 806 | 读取用于手持设备的超帧 |
| | 807 | 请求用于手持设备的超帧 |
| | 784 | 读取链路列表 |
| | 967 | 写入链路 |
| | 968 | 删除链路 |
| | 786 | 读取邻居属性标志 |
| | 971 | 写入邻居属性标志 |
| 管理图路由和源路由 | 802 | 读取路由列表 |
| | 974 | 写入路由 |
| | 975 | 删除路由 |
| | 785 | 读取图列表 |
| | 969 | 写入图的有向边 |
| | 970 | 删除图的有向边 |
| | 803 | 读取源路由 |
| | 976 | 写入源路由 |

（续）

| 分　类 | 命　令　号 | 描　　述 |
|---|---|---|
| 安全 | 961 | 写入网络密钥 |
| | 782 | 读取会话列表 |
| | 963 | 写入会话 |
| | 964 | 删除会话 |
| | 823 | 请求会话 |
| | 814 | 读取设备列表实体 |
| | 815 | 添加设备列表实体 |
| | 816 | 删除设备列表实体 |
| | 821 | 写入网络接入模式 |
| | 822 | 读取网络接入模式 |
| 带宽管理 | 799 | 请求时间表 |
| | 800 | 读取时间表的列表 |
| | 801 | 删除某个时间表 |
| | 973 | 写入某个时间表 |
| | 812 | 读取数据板的接收优先级 |
| | 813 | 写入数据板的接收优先级 |
| 设备管理 | 960 | 使设备从网络中断开 |
| | 972 | 暂停设备 |
| | 777 | 读取无线设备能力 |
| | 778 | 读取电池寿命 |
| | 793 | 写入 UTC 时间的映射 |
| | 794 | 读取 UTC 时间的映射 |
| 网络维护 | 795 | 写入时间间隙 |
| | 796 | 读取时间间隙 |
| | 808 | 读取数据板的生存时间 |
| | 809 | 写入数据板的生存时间 |
| | 810 | 读取入网优先级 |
| | 811 | 写入入网优先级 |
| | 819 | 读取退避指数 |
| | 820 | 写入退避指数 |

（续）

| 分　类 | 命令号 | 描　述 |
|---|---|---|
| 共存 | 804 | 读取CCA模式 |
| | 805 | 写入CCA模式 |
| | 817 | 读取信道黑名单 |
| | 818 | 写入信道黑名单 |
| 网络健康报告和状态 | 779 | 报告关于设备通信统计的设备健康 |
| | 780 | 报告邻居设备的健康列表 |
| | 787 | 报告邻居设备的信号等级 |
| | 788 | "路径失效"报警 |
| | 789 | "源路由失效"报警 |
| | 790 | "图路由失效"报警 |
| | 791 | "传输层失效"报警 |
| 网关命令 | 832 | 使用HART设备唯一的ID读取该网络设备的标识 |
| | 833 | 读取网络设备的邻居设备健康情况 |
| | 834 | 读取网络拓扑信息 |
| | 835 | 读取突发报文列表 |
| | 836 | 清除网关缓存中某个设备发出的命令响应 |
| | 837 | 向某设备写入更新通知标志位 |
| | 838 | 读取某设备的更新通知标志位 |
| | 839 | 改变通知 |
| | 840 | 读取网络设备的统计信息 |
| | 841 | 读取使用昵称的网络设备标识 |
| | 842 | 写入网络设备的调度标志 |
| | 843 | 读取网络设备的调度标志 |
| | 844 | 读取网络约束 |
| | 845 | 写入网络约束 |

3. 命令状态字节

从节点的所有响应报文必须在其数据字段的前两个字节中返回两个字节的命令状态。第一个字节是多元的，其包含了通信状态或响应代码。第二个字节总是包含现场设备的状态。

## 5.2 动态和设备变量

HART 协议被设计为支持智能现场设备技术和 4~20mA 回路电流。HART 命令 1 和命令 2 可以返回主要变量（Primary Variable，PV）、回路电流和百分比量程。HART 命令 3 除了能返回命令 1 和命令 2 能返回的值外，还可以返回次要变量（Secondary Variable，SV）、第三级（Tertiary Variable，TV）和第四级（Quaternary Variable，QV）变量。这些变量被统称为动态变量。HART 命令 9 最多允许返回 8 个数字量。HART 命令 9 也可以包括一些状态信息和一个标示测量发生时的时间戳。

此外，HART 协议支持的设备变量可用于更精密的智能现场设备和多变量现场设备。而且，多变量现场设备能配置设备变量以接入到电流回路。

## 5.3 上位机一致性等级

上位机一致性等级按照上位机功能水平标识出上位机的能力。这个上位机功能包含上位机能提供的数据访问和操作的水平，并包括对常规命令和设备族命令的访问。每个一致性等级涵盖了所有较低等级的功能。等级 1 是最小的等级，其能够被任何上位机应用拥有。表 5-3 列出了这些等级。

表 5-3 上位机一致性等级

| 等级 | 描述 |
|---|---|
| 0 | 上位机没有满足一致性等级 1 的最小需求 |
| 1 | 上位机可以利用任何现场设备的循环过程数据 |
| 2 | 上位机能够为用户提供关于任何现场设备的基本识别和配置数据 |
| 3 | 上位机能够执行任何设备的基本配置。最低级别被归类为“通用上位机” |
| 4 | 上位机能够为任何设备提供基本的调试和校准服务 |
| 5 | 上位机能够访问所有现场设备的数据项，并能够访问现场设备中的所有设备特定命令 |

# 第6章 WirelessHART网络

摘要：一个WirelessHART网状网络是由多种不同设备组成的。WirelessHART网络中大部分节点是用于收集工业过程数据或控制工业过程的某些现场设备。WirelessHART网络中的所有设备都具有路由功能，其中一些设备可能只扮演路由器的角色。接入点是在网关与所有其他设备之间的路由器。接入点与网关之间的通信被假设为可靠的、不占用无线带宽的。网关是无线网络和上位机之间的接口，也是整个网络和网络管理器之间的桥梁。网络管理器主要负责控制新节点入网、配置网络、维护网络以及其他所有网络管理任务。安全管理器的一个主要职责是负责管理网络层和数据链路层的密钥。WirelessHART标准还定义了两种特殊的网络设备：WirelessHART适配器和手持设备。WirelessHART适配器在有线HART网络中扮演着上位机的角色，为有线HART设备提供无线通信服务。手持设备通常被工业现场操作员携带，用于工业现场的日常维护和故障处理。手持设备不像其他WirelessHART设备，其主要被用于移动环境中，并且能够与多个网络或设备相连。请参照HART标准中“无线设备规范（HCF_SPEC-290）”以获得更详细的信息。

WirelessHART产品将被分为5种不同类型：现场设备、适配器、手持设备、网关和网络管理器。其他的设备类型将可能在后续版本中发布。

第1章中的图1-2展示了一个通过一个网关连接到工厂自动化网络的WirelessHART网络。该工厂自动化网络可以是一个基于TCP的网络、一个远程IO系统，或者一个现场总线（如PROFIBUS™ DP）。该网关通过WirelessHART接入点接入到WirelessHART网络。

所有与WirelessHART网络直接相连的设备都可被归纳成一类设备——WirelessHART网络设备。WirelessHART网络设备包括WirelessHART现场设备、WirelessHART适配器、WirelessHART路由器、WirelessHART接入点和WirelessHART手持设备。

所有WirelessHART网络设备都可以发送和接收WirelessHART数据报，以及执行一些基本功能以支持WirelessHART网络的形成和维护。所有WirelessHART网络设备必须能够产生和汇集WirelessHART数据报，并且能够为网络中的其他网络设备路由数据报。

## 6.1 WirelessHART 现场设备

WirelessHART 现场设备被连接到工业过程上用来测量或者控制工业过程。它们是 WirelessHART 数据报的产生者或消费者，并必须能够为其他网络设备路由数据报。

WirelessHART 现场设备可以广泛地使用在各种应用领域，例如监测和控制罐内液面、监测排放水平和水量、监测设备健康等各种各样的监控应用。WirelessHART 现场设备还可以测量温度、压力、流量、pH、密度、成分、排放水平、振动等。它们也可以连接到一些终端控制设备，如阀门、搅拌机、鼓风机和传送带。

WirelessHART 现场设备的供电方式可以是有线电源、回路电源、电池或其他方式。终端现场设备可被直接连接到工业过程或工厂设备。WirelessHART 现场设备可能支持或不支持传统的电流回路信号，但是它们都必须拥有一个维护端口用于设备配置和本地诊断。WirelessHART 设备并不要求提供有线的 4 ~ 20mA 信号。

### 6.1.1 一般要求

所有 WirelessHART 现场设备必须支持所有 HART 通用命令、一些 HART 常规命令以及针对 WirelessHART 设备定义的标准化的命令和程序。

### 6.1.2 维护端口

所有 WirelessHART 现场设备必须提供一个符合令牌传送数据链路层规范（Token-Passing Data Link Layer Specification）的维护端口。这个维护端口必须支持至少一个 HART 标准定义的物理层。这个端口被用于设备配置和维护（例如，给设备配置入网密钥和网络标识符、或者监视设备入网过程）。

连接到维护端口的手持设备和资产管理应用程序都不能访问 WirelessHART 网络。

### 6.1.3 WirelessHART 设备接口

WirelessHART 现场设备首先是个 HART 设备。所以，WirelessHART 现场设备必须遵守所有 HART 设备的要求，同时也必须遵循所有 WirelessHART 标准的要求。作为设备规范的一部分，WirelessHART 现场设备必须支持所有常规命令。

此外，作为设备规范的一部分，WirelessHART 现场设备必须支持状态（Status）和扩展状态（Extended Status）。状态提供了对测量质量的一个指示，以判断正在进行测量的设备是否健康以及测量结果是否及时。设备检查与输入输出相关的硬件和

软件，并相应地将这些结果通过状态值的方式显示。计算后的输出参数状态给出了明确的量值指示：好的值、差的值、坏的值或固定的常量值。好的状态值可能被用于控制；差的状态值是可疑的，因为其可能没有反映出真实的测量值或计算值。糟糕的状态值意味着它没有反映出真实的测量、计算值或控制值。固定的状态量值意味着参数值是一个常量，且没有被周期性地更新。状态也反映了一些其他的额外信息，如配置的变化、冷启动、回路电流固定、回路电流饱和、非主要变量超出范围以及主要变量超出范围。

扩展设备状态量能提供以下一些信息：设备是否出故障了（需要维护）、设备变量是否处于报警或警告状态（设备变量警报），或者设备的电源是否非常低（严重电源失效）。设备状态和扩展设备状态都作为一部分被包含在突发模式通信中。

WirelessHART 标准中的另一个重要特色是每个值都有一个时间戳。附加的时间戳可以让应用程序确定这个参数有多新、测量过程是否有抖动以及在某些情况下使用时间值和测量值来决定适当的控制操作。

现场设备还支持另外三种主要的特色服务：突发模式（Burst Mode）、块数据传输（Block Data Transfer）和事件通告（Event Notifications）。突发模式用于在特殊情况下发送数据。块数据传输用于在设备与上位机之间传输一个数据块，例如一个频谱分析数据。事件通告发布设备状态的变化，它与其他突发模式支持的数据发布相互独立。

现场设备的一个关键特色是它们具有被安装和使用于各种各样应用场合的能力。实际的工业过程要求被安装的现场设备能够被组态。作为组态的一部分，现场设备将被给予一个标签、标定（仪器标定包括高量表值、低量表值、工程单元和小数位）以及应用的信号调节（如果设备是一个阀门，那么当信号值增加的时候，知道阀门向哪个方向移动是非常重要的）。现场设备的调试和校准可能在生产工厂中进行，也可以在仪表车间中进行，或者在仪表被安装了以后进行。EDD 文件描述了设备支持的参数集和可以使用的方法。EDD 文件用 EDDL 表述。终端用户通常有一些针对不同类型设备的标准参量模板，然后它们可以利用这些模板来对在工厂里使用的设备进行定制（很多都是使用基于 EDD 文件的工具）。这样，设备就能完全被离线定义，并在工厂、商店或者启动之前通过下载离线组态信息到被组态设备，从而实现设备的组态。用户所需要做的就是将唯一设备标识符关联到组态系统中，并使用这个标识符作为设备的密钥。

突发模式、块数据传输、维护和组态、时间通告都需要占用网络资源。为此，WirelessHART 标准支持设备、上位机和网络管理器具备请求网络服务和带宽的功能。在 WirelessHART 标准中，我们利用时间表来定义和描述这些请求服务。

## 6.2 WirelessHART 路由设备

WirelessHART 路由设备是一种能为一个网络设备转发数据报到另一个设备的网络设备。担任路由器功能的 WirelessHART 网络设备使用其图和连接以决定发送数据报给哪个邻居设备。通常，因为所有 WirelessHART 网络设备都必须支持路由功能，所以独立的 WirelessHART 路由器是不需要的。但是，布置一些额外的 WirelessHART 独立路由器以改善网络路由，这样是有益的（例如扩展网络或者节省网络中 WirelessHART 现场设备的能耗）。这些 WirelessHART 独立路由器不直接接入到工业过程，也不扮演网关的角色。

在某些情况下，安装一个额外的 WirelessHART 接入点比安装一个额外的 WirelessHART 路由器更好。WirelessHART 接入点能提高整个网络的吞吐量和实现网络冗余。

## 6.3 WirelessHART 适配器

WirelessHART 适配器可以与 HART 现场设备相连、或者与几个多点通信的现场设备相连。这样，HART 现场设备之间就可以通过 WirelessHART 网络进行通信。WirelessHART 适配器必须包含一个有线的令牌传递接口和一个无线的 TDMA 接口。换句话说，除非另有说明，WirelessHART 适配器必须满足有线 HART 和 WirelessHART 通信的所有要求。此外，由于连接到 WirelessHART 适配器的 HART 现场设备可能是早期版本的，所以 WirelessHART 适配器必须为了这些附属的子设备而支持 HART 7 版本中的一些关键功能，例如 WirelessHART 适配器必须支持至少 5 个突发模式报文和 2 个事件报文。

WirelessHART 适配器也必须能够完全访问其附属子设备的组态信息和状态信息。WirelessHART 适配器除了支持与其附属现场设备之间的 HART 通信，还必须做到不能对 HART 设备的模拟信号造成不利影响。

WirelessHART 适配器必须支持 HART 通用命令和 HART 常规命令，并通过身份命令响应来识别自己。此外，WirelessHART 适配器还必须支持至少一个块数据传输连接。

WirelessHART 适配器为自己以及附属子设备请求网络资源。在许多情况下，例如当一个搜索广播被发送出去时，WirelessHART 适配器必须能够代表其附属子设备响应该搜索广播。

## 6.4 手持设备

手持设备被用于网络设备的安装和维护。手持设备是被工厂人员操作的便携式设备。与手持设备的连接方法总共有以下四种：

（1）通过工厂自动化网络连接的 HART 手持设备或应用程序　一个能与工厂自动化网络相连的手持设备，可以通过某些网络技术（如 WiFi）与工厂自动化网络相连。像外部工厂自动化服务器一样，这类手持设备通过网关来实现与 WirelessHART 网络设备的通信。对于 WirelessHART 网络而言，这类手持设备就像另一个上位机。

（2）通过 FSK 模块与设备相连的 HART 手持设备　在这种模式中，手持设备通过一个 FSK 模块直接与设备相连。在这种模式下，手持设备不能通过与其相连的设备来访问 WirelessHART 网络。

（3）连接到 WirelessHART 网络的 WirelessHART 手持设备　在这种模式中，WirelessHART 手持设备是 WirelessHART 网络中的一种设备，像其他 WirelessHART 网络设备一样被部分限制，例如只能与网络管理器和网关通信。这种模式用来给无线手持设备配置密钥，以及读取诊断和系统健康信息。这种模式也被称为作为网络设备来连接。

（4）连接到 WirelessHART 现场设备的 WirelessHART 手持设备　如果一个基于 WirelessHART 连接的手持设备通过 WirelessHART 网络连接到一个 WirelessHART 设备，那么它将被限制为只能与其相连的设备进行通信。我们将采用特殊的配置来确保 WirelssHART 手持设备被限制为每次只能与直接相连的设备进行通信。这个被称为作为维护设备来连接。在这种方式下工作的手持设备必须利用自己与相连设备之间的会话来进行通信。

## 6.5 WirelessHART 网关和接入点

WirelessHART 网关和接入点可以把 WirelessHART 网络与工厂自动化网络连接起来，并允许这两种网络之间的数据交互。上位机可通过 WirelessHART 网关设备来访问 WirelessHART 网络设备。网关设备能用于两个不同网络间的协议转换，像中间人一样使两个或更多不同协议的网络看起来像同种协议的网络，并且还能实现命令和数据的格式转换。WirelessHART 网关的主要功能还包括缓存从现场设备传送来的突发数据，然后将这些数据发送给上位机。缓存功能不仅提高了 WirelessHART 网关对于上位机的响应速度，还极大地减少了网络通信量。如果只发送异常变化的数据，那么 WirelessHART 网络通信量通常可以减少为 1/10 ~ 1/20。

在很多情况下，WirelessHART 网络会有多个 WirelessHART 接入点。多个 WirelessHART 接入点能被用于提高 WirelessHART 网络的有效吞吐量和可靠性。WirelessHART 接入点直接与 WirelessHART 网关通信。

一个 WirelessHART 网络的部署包括安装 WirelessHART 现场设备、一个 WirelessHART 网关（在许多情况下包括一个 WirelessHART 网关和多个 WirelessHART 接入点）以及和上位机或控制系统的连接。一旦 WirelessHART 网关、WirelessHART 现场设备、控制系统被组态好了，WirelessHART 网状网络就能自动形成并开始通信。

为了简化对冗余接入点的支持，每个 WirelessHART 网关都有一个固定的、众所周知的地址（唯一 ID =0xF981000002；昵称 =0xF981）。每个 WirelessHART 网络至少有一个 WirelessHART 网关，同时还可以有冗余的 WirelessHART 网关。

### 6.5.1 一般要求

WirelessHART 网关使用标准的 HART 命令来与 WirelessHART 网络设备以及上位机通信。WirelessHART 网关也扮演着服务器的角色，其收集、维护和缓存来自于 WirelessHART 网络设备的数据和命令响应。这些缓存的响应包括突发信息、事件通告和普通的命令响应。这样就可以降低 WirelessHART 网络的通信量，减少 WirelessHART 网络设备的能耗，以及提高上位机的响应速度。

WirelessHART 网关必须能够本能地支持 WirelessHART 适配器透明地访问其附属的子设备。WirelessHART 网关通过轮询 WirelessHART 适配器的方式来识别出该适配器的附属子设备。首先，WirelessHART 网关使用命令 74 来确认有多少个子设备被连接到 WirelessHART 适配器。然后，WirelessHART 网关再通过命令 75 来遍历轮询地址、IO 卡和信道标识符的组合，直到所有连接的子设备都被识别到。

如果 WirelessHART 网关支持多个 WirelessHART 接入点，那么网络管理器将在每个 WirelessHART 接入点上都分配一定的通信量。如果这些 WirelessHART 接入点中的某个接入点失效了，那么网络管理器将调整调度分配，使通信流量分散到其余的 WirelessHART 接入点。每个 WirelessHART 接入点都有自己的物理地址和昵称地址。

所有 WirelessHART 接入点都通过 WirelessHART 网关把数据传送给上位机接口或网络管理器。WirelessHART 网关必须为其他 WirelessHART 网络设备提供网络时钟。时钟信息从 WirelessHART 网络层次结构的顶端（网关处）向下扩散至最底端。

### 6.5.2 WirelessHART 网关模型

WirelessHART 网关用于将 WirelessHART 网络与其他网络（如工厂自动化网络）相连，并允许两个不同网络之间交互 HART 命令/响应、隧道信息、XML 格式

数据和诊断信息。WirelessHART 网络使用了网关的概念来提供一个单一的 WirelessHART 网络实体接口。服务接入点提供到上位机接口的访问，WirelessHART 接入点提供到 WirelessHART 网络本身的访问。

1. WirelessHART 网关

WirelessHART 网关提供了一个到 WirelessHART 网络的单实体接口。

1）它是 WirelessHART 网络的一部分：①它是 WirelessHART 网络中的一种设备类型；②它通过 WirelessHART 接入点与其他 WirelessHART 现场设备通信（WirelessHART 网关必须与 WirelessHART 网络中的任何一个设备都有一条可达路径）。

2）它能与网络管理器直接通信。

3）它能作为时钟源发布时间同步信息。

4）它是一种 HART 设备类型：①由设备描述语言（Device Description Language，DDL）描述；②支持 HART 设备描述。

5）它支持一个或多个服务接入点以连接自动化网络和工厂骨干网络。它能通过这些服务接入点支持以下功能：①使 HART 命令满足当地缓存数据的转换功能。WirelessHART 网关执行数据缓存以优化 WirelessHART 网络综合性能，并提高对上位机的响应速度；②将 HART 命令转化成 WirelessHART 网络请求的隧道功能。WirelessHART 网关能通过不同物理层（RS-485，Ethernet LAN，Wi-Fi 等）并基于各种协议（例如 Modbus，Profibus DP，ControlNet，HART OPC server，proprietary 等）与上位机通信；③可选地支持基于 XML 的接口。

6）兼容性：WirelessHART 网关可以支持已有的 HART 命令（仅限于该网关充当翻译者或代理者时）。

7）它为以下服务提供缓存：①突发模式；②事件通告；③缓存的命令响应；④诊断；⑤大块数据传输（几种具体案例在 WirelessHART 标准制定的过程中常被用到，例如网关从设备接收数据的两个应用案例有：一个阀门上传其重要信息，一个振动分析仪返回其测量结果；网关也能实现将大块数据/文件向下转发给设备）。

8）它提供了把变量发布到设备的功能（常被称为抓取的变量）。在这种情况下，WirelessHART 网关能将缓存的突发模式数据发布给 WirelessHART 网络中其他的网络设备。

靠近上位机的网络可能使用各种各样的网络技术。大多数 PLC、DCS 或 SCADA 制造商都使用一个专有网络。然而，资产管理和设备管理公司则倾向于使用开放协议，例如 TCP/IP 和一些 MAC/PHY 层标准（IEEE 802.11™和 IEEE 802.3™）之一。

2. WirelessHART 接入点

WirelessHART 接入点是一种位于 WirelessHART 网关和 WirelessHART 网络之间

的网络设备。WirelessHART 接入点的一边与 WirelessHART 网络相连，另外一边是一个外部连接。这个外部连接可以是一个以太网、Wi-Fi 网络或一个专有网络。WirelessHART 标准并没有规定这种外部连接。WirelessHART 接入点不能直接与工业过程相连。我们对 WirelessHART 接入点有以下几点说明：

它们是 WirelessHART 现场设备网络的一部分：①它们是 WirelessHART 网络中的一种设备类型；②它们通过专用链路或通信端口与网关通信；③只要网络管理器提供路径，每个 WirelessHART 接入点都能与任何 WirelessHART 设备通信。

3. 服务接入点

服务接入点（Service Access Point，SAP）能提供到自动化网络和工厂骨干网络的连接。它们能提供以下功能：

1）为欲访问 WirelessHART 网络设备的上位机系统或应用程序提供到网关的接口。通过该接口，上位机系统或应用程序能访问所有带有 WirelessHART 适配器的有线 HART 设备。

2）访问缓存的响应报文：①突发模式响应；②事件通告响应；③缓存命令响应。

3）访问诊断信息。

4）访问网络管理器的数据。

5）为块数据传输提供支持（例如上传振动分析仪的数据）。

6）将 HART 命令转化成 WirelessHART 网络和 WirelessHART 设备请求的隧道功能。通过这些服务接入点，网关能通过不同物理层（RS-485，Ethernet LAN，Wi-Fi 等）并基于各种协议（例如 Modbus，Profibus DP，ControlNet，HART OPC 服务器以及专有协议等）与上位机相连。

两种类型的接口被用以支持服务接入点。第一种接口直接支持 HART 命令，所有 WirelessHART 网关都必须支持该接口。第二种接口支持 XML 格式的命令，不过 XML 接口是可选的。

4. 隧道协议

WirelessHART 网关也必须能支持隧道协议。WirelessHART 网络外的上位机可以利用隧道协议来与 WirelessHART 网络内部的目标设备传递报文。所有 WirelessHART 网关都必须能支持 HART 和 WirelessHART 通用命令和常规命令，同时它们也可能支持厂商自定义的命令。

WirelessHART 网关支持的隧道协议包括：WirelessHART 协议、基于以太网的 HART 协议、如 TCP/IP 的开放协议和厂商自定义的协议。

5. 上位机

上位机接口用于将 WirelessHART 网络外的客户端与 WirelessHART 网络中的设备相连接。上位机接口有多种形式，其中包括以下几种常见的形式：

1）以太网到 WirelessHART 网络的网关设备：一种在工业以太网和 WirelessHART 网络之间提供双向路径的网关设备。

2）WiFi 网络到 WirelessHART 网络的网关设备：它是以太网到 WirelessHART 网络的网关设备的一种变体。它使用 802.11 a/b/g 无线技术连接到工厂网络。

3）串口到 WirelessHART 网络的网关设备：如果工厂自动化服务器和设备支持串口连接，那么串口到 WirelessHART 网络的网关设备能被用来与这些设备的串口互联。

WirelessHART 网关必须能缓存突发模式命令、几种常用读写命令以及诊断。为了利用这个缓存功能，网关也必须能充当命令解析器的角色。作为一个命令解析器，网关检查上位机发来的请求，如果对应的响应数据已被缓存并仍然有效，那么网关将从自己的实时数据库中取出缓存的响应报文并返回给上位机。例如，如果某个上位机上的客户端向 WirelessHART 网络中的某个设备发布 HART 命令 0 的请求，网关将查看其是否缓存有 HART 命令 0 对应的响应数据。如果网关没有 HART 命令 0 对应的响应数据，那么它将把这个 HART 命令 0 转发给相应的设备，然后再把得到的响应数据返回给该客户端。

命令解析器功能可能相当复杂。网关能处理网络层和一些应用层的交互。在网络层，命令解析器必须能处理不同长度的响应数据报，还需要处理安全、优先级、地址等的映射。

6. 缓存的响应报文

1）网络状态：每个网络设备都维护着一些诊断信息。这些诊断信息通过 HART 命令周期性地发布给网络管理器。网络管理器维护着所有设备和整个网络的诊断信息。上位机可以通过查询网关或者网络管理器来获得网络诊断报文。

2）突发模式命令响应：数据库缓存了所有突发模式的响应报文。

3）事件通告命令响应：数据库缓存了所有事件通告的响应报文。

4）缓存的命令响应：数据库缓存了几种命令的最新响应报文（这些命令汇总如下）。

5）延时的响应命令响应：对于 HART 请求/响应命令，网关维护着一张包含所有未完成命令的完整列表。这些未完成的命令是已经被发送给设备但还没有收到响应的命令。如果延时的响应命令存储时间超过 24h，那么它们必须被清除掉。

## 6.6　网络管理器和安全管理器

网络管理器也可被认为是一种网络设备。这样，其他 HART 设备与网络管理器之间就能被允许交互 HART 命令。本节将详细地描述网络管理器。

网络管理器负责所有 WirelessHART 网络的管理、调度和优化。作为其职责的一部分，网络管理器还负责初始化和维护网络通信的参量值。网络管理器提供各种机制来支持设备的加入和离开网络，也负责管理专用的和共享的网络资源。

网络管理器通过“网络管理规范”定义的网络层与 WirelessHART 网络设备通信。“常规命令规范”和“无线命令规范”定义了网络管理器用来建立、监测和管理整个网络的命令。网络管理器也负责收集和维护关于整个网络健康的诊断信息。这些诊断信息可被报告给上位机，也可被用来相应的调整网络以适应外界环境的变化。

为了实现其所有功能，网络管理器需要 WirelessHART 等设备的信息、如何使用网络的信息以及网络运行性能的反馈信息。设备的配置和安装信息是从设备自身读出的。通信资源是由设备、应用和用户自行申请。网络运行状况的反馈是由设备以健康报告和诊断信息的形式提供给网络管理器的。

用户（管理员/维修员）可以与网络管理器应用进程进行交互来产生一个网络管理控制包，并将该包发送给网络设备。网络管理控制包途经 WirelessHART 接入点的网络层、数据链路层、物理层，直到被无线发送给目标设备。

### 6.6.1 核心网络功能

（1）网络管理器　网络管理器负责 WirelessHART 网络的形成、配置新网络设备、让新网络设备加入网络以及监测网络。网络管理器还可以利用诊断信息持续不断地调整网络拓扑结构，这些调整可被称为修改和梳理网络。WirelessHART 网络体系结构并不限定网络管理器在工厂自动化网络的位置。如第 1 章中的图 1-2 所示，网络管理器可能与网关共存于一个盒子里，或位于完全独立的物理盒子里。每个 WirelessHART 网络都有一个网络管理器，而一个网络管理器可以管理多个 WirelessHART 网络。

（2）网络管理器和安全管理器的连接　安全管理器和网络管理器需要在彼此间建立一个连接，并维护这个连接以支持设备入网请求和建立会话。WirelessHART 标准并不定义安全管理器和网络管理器间的连接方式及安全方式。安全管理器与网关之间没有直接联系。

（3）安全管理器　安全管理器与网络管理器协同工作以保证 WirelessHART 网络免受敌对威胁。安全管理器产生和管理 WirelessHART 网络所用到的密码信息，也负责产生、存储和管理各种密钥。安全管理器与网络管理器之间的工作模式是服务器-客户模式。安全管理器独立于网络管理器的原因是：在一些涵盖多个 WirelessHART 网络的工厂自动化网络中，安全管理器可能是一种集中式的机体，即一个安全管理器可以与每个 WirelessHART 网络相联系。网络管理器与安全管理器间的连接必须是安全的，但是该安全连接的定义也不在 WirelessHART 标准的范围

之内。

（4）网络诊断 作为其系统功能的一部分，网络管理器收集 WirelessHART 网络性能和诊断信息。在网络运行期间，这些获取的信息使得观察和分析 WirelessHART 网络行为成为可能。如果发现问题，对 WirelessHART 网络的重新配置将在网络运行的同时被执行。WirelessHART 网络的诊断信息可以通过 HART 命令来得到。

（5）网络性能 WirelessHART 网络通过多种机制来确保很高的可靠性。这些机制包括：多条路径到网络设备、多 RF 信道以及重传机制。如果期望更高的网络可靠性，可以通过增加额外的 WirelessHART 接入点和 WirelessHART 现场设备来形成更多的路由路径。额外的设备增加了路径的多样性。额外的 WirelessHART 接入点和设备同时还能增加 WirelessHART 网络的吞吐量、减少延时，以及被用于路由以绕过潜在的干扰源。

（6）时间同步 WirelessHART 网络的所有通信都是时间同步的。WirelessHART 网络的时间度量单位是时间长度固定的时隙。时隙被所有网络设备共享。一个时隙的时间足够用来在一个信道发送或接收数据报以及相应的确认数据报，还包括用于网络同步的保护带时间。在同一个时隙上可以同时发生多个通信。

精确的时间同步对基于时分多路复用的网络来说至关重要。因为所有的通信发生在时隙中，所以网络设备都必须以最小偏差地知道每个时隙的开始和结束时间。WirelessHART 标准定义了时间同步的机制。在 WirelessHART 网络中，基准时间信息是从 WirelessHART 网关向外地逐步传播的。

（7）会话 网络层的会话管理着端到端的通信。每个会话包含了一对（或一组）网络设备的安全信息。所有网络设备与网络管理器之间都将有两个会话：一个会话是为了它们之间的点对点通信，另外一个会话是用于管理从网络管理器来的网络广播通信。所有的网络设备还需要有两个网络管理器会话密钥。会话由分配给网络设备的地址来区分。对于与网络管理器的点对点会话，我们使用标准的网络设备地址；对于广播会话，我们使用一个特殊的网络设备地址 0xFFFF。

（8）网关和网络管理器的连接 WirelessHART 标准没有描述网关与网络管理器间的接口。网络管理器和网关负责在彼此间建立一个安全的连接，并且维护这个连接以传递控制信息和数据。这样，网关就没有必要经历普通网络设备所必须经历的入网过程。一旦网关连接到网络管理器，网络管理器就可以配置网关使其开始向其他设备广播信息。一旦网络管理器为上位机和现场设备之间建立起了通信路径，那么网络管理器将不会再干涉上位机和网络设备之间应用数据的通信。网关负责缓存数据、协议转换、超时、维护网络时钟等。

（9）调度　网络管理器的主要职能是调度、监测、管理和优化通信资源。网络管理器将网络拓扑结构、通信需求以及从网络设备和应用程序发出的通信资源请求等信息结合起来产生调度。

### 6.6.2　网络管理需求

网络管理器是整个 WirelessHART 网络运行的核心。网络管理器负责网络的形成、建立路由、调度通信资源、检测网络健康状况、根据网络的变化进行相应调整以及与安全管理器合作来分配和管理会话密钥。表 6-1 汇总了网络管理器的需求。

**表 6-1　WirelessHART 网络管理器的需求**

| 网络功能 | 需　求 |
|---|---|
| 网络形成和组态 | 提供初始化和启动网络的解决方案 |
| | 管理网络的拓扑结构。理解网络拓扑结构。基于网络设备报告的诊断信息，相应地调整网络 |
| | 管理网络密钥。网络密钥首先由安全管理器提供给网络管理器，然后等管理器再将网络密钥提供给所有的网络设备。网络管理器负责分发网络密钥，并根据工厂安全政策的要求来周期性地更新网络密钥<br>网络管理器和网关使用不同的密钥用来单播或广播自己发出的数据报 |
| | 管理设备入网过程。网络管理器负责验证欲加入网络的设备。在对入网设备进行认证后，网络管理器向该入网设备分发 1 个网络密钥和 4 个会话密钥。这 4 个会话密钥的具体用途如下：<br>1）网络管理器单播会话密钥<br>2）网络管理器广播会话密钥<br>3）网关单播会话密钥<br>4）网关广播会话密钥<br>入网设备还需要被分配一个网络 ID 来正确地发现目标网络 |
| | 分配一个 16 位的昵称。网络管理器为每个网络设备分配和管理一个唯一的 16 位网络昵称（网络地址）。网络管理器负责确保每个设备内部的邻居表都是最新的 |
| | 建立一个与网关的连接。无论何时，只要网关（或通过网关的接入点）接收到目标地址是网络管理器的数据报，网关都需将这些数据报转发给网络管理器 |
| | 为网关配置至少一个的 WirelessHART 接入点以便提供网络时钟 |
| | 管理网络配置。维护一幅完整的网络配置图，其中包括任何已分发给网络设备的与网络相关的信息 |
| | 响应对网络信息的请求。例如，当一个上位机请求网络中所有网络设备的信息时，网络管理器负责提供该响应 |

（续）

| 网络功能 | 需求 |
| --- | --- |
| 路由 | 创建和管理网络路由。网络路由是一幅完整的网络图 |
| | 管理邻居表。网络管理器通过设备的周期性健康报告来收集网络统计信息和邻居表信息。网络管理器利用这些信息对网络做出一些适当的调整 |
| | 为图路由建立路由表。图路由对于上传和下传通信都是很理想的。上传通信包括过程测量和警报，下传通信包括对执行器的 SP 变化 |
| | 为源路由建立源路由列表 |
| | 为自己、网关和网络设备分配通信资源，以便网络管理器能管理网络，同时也使得网络设备能彼此通信 |
| 网络调度 | 创建超帧。多超帧被用于支持不同频率的通信。另外，可以为一些特殊的设备管理和诊断应用程序分配额外的超帧。这些应用程序通常要求在短时间内发送大量的数据报 |
| | 分配超帧中的链路 |
| | 创建链路表。每个链路都包括了一个与某超帧关联的时隙、链路类型（普通、广播、发现、加入）、链路选项（发送的、接收的、共用的）、邻居信息、信道偏移以及连接到该链路的设备 |
| | 根据应用程序的要求激活或停用超帧 |
| | 管理整个 WirelessHART 网络的诊断信息。例如，当一个网络设备在 Keep-AliveInterval 期间没有收到其邻居设备发来的数据报时，它将发送一个断路（path-down）通知给网络管理器以表明该路径已不可用 |
| 网络调度和信道管理 | 跟踪和记录列入黑名单的信道（黑名单是一种手工操作） |
| | 提供信道偏移。信道偏移用来在信道跳转时计算通信的信道号。信道偏移取值范围为 0 到最大可用信道数，最大可用信道数为信道数减去黑名单信道数 |
| 网络诊断和适应 | 维护和记录每个网络设备的健康信息 |
| | 根据环境变化和应用请求来调整网络，包括更新路由和调度信息 |
| | 根据网络设备的请求来分配通信资源。网络设备请求网络带宽来支持突发模式、时间通告和块模式数据传输。网关请求网络带宽来支持客户端请求。增加或者减少通过某个特殊设备的连接数，从而使网络数据量偏向到某个特殊的路径上 |
| | 优化路由和调度以改善网络性能和节省设备能量 |
| 安全管理器 | 创建和管理入网密钥 |
| | 创建和管理会话密钥 |

### 6.6.3 调度

网络管理器最重要的功能是调度通信资源。为了实现既有效又最佳的调度，网络管理器需要知道 WirelessHART 网络信息、通信需求信息、网络设备能力信息等。当获得这些信息后，网络管理器可以不断地调整通信调度直到满足 WirelessHART 网络的需求。最后，调度器还可以通过系统运行中的反馈来微量调整调度。

调度需求

表 6-2 汇总了 WirelessHART 网络调度器的一些需求。

**表 6-2 WirelessHART 网络调度器的需求**

| 功　能 | 需　求 |
|---|---|
| 假设 | 网络管理器能合理地表现网络的图路径 |
| | 每个设备被配置了一个连接表 |
| | 网络管理器知道每个网络设备的更新率 |
| | 为了提供冗余，一个数据报需要在一条路径上被分配一次发送和一次重传，还需要在另外一条路径上被分配另一次重传 |
| 约束条件 | 可同时使用的最大信道数由可用信道数决定（由黑名单限制） |
| | 设备不能被调度成在一个时隙内侦听两次 |
| | 多个设备能同时给同一个设备发送数据（例如，对于每个接收状态的设备，一个广播链路和一个专用链路能共存） |
| | 在多跳路径上，前面的跳必须先被调度 |
| | 支持的更新率应该被定义成 $2^n$ 的格式，其中‘$n$’可以为正整数或负整数。例如，更新率可为¼（即 250ms）、½（即 500ms）、1（即 1s）、2（即 2s）、4（即 4s）、8（即 8s）、16（即 16s）、32（即 32s）、60（即 60s）或更多 |
| | 基本的网络管理通信和突发模式通信不应该超过可用通信带宽（最多 100 时隙/s）的 30% |
| | 服务：网络管理器必须考虑服务请求 |
| | 最终的调度结果（不包括网关）应该有 50% 的空闲时隙（用于分配给重传、接收等） |
| 数据超帧 | 数据超帧的长度由数据的扫描率决定 |
| | 根据扫描率由快到慢来分配时隙 |
| | 从最远端设备到网关的每个中间路由设备都需要被分配一个链路。在相同的路径上再分配另外一个专用链路用于重传。同时，在另外的一个路径上分配一个分享链路来处理第二次重传 |

（续）

| 功　　能 | 需　　求 |
| --- | --- |
| 管理超帧：管理 | 管理超帧的优先级高于数据超帧 |
| | 从网关开始用宽度优先搜索遍历图，标记设备为 $N_0$，$N_1$，… $N_n$ |
| | 每个设备最少需要一个时隙用来发送“Keep-Alives”报文，同时在其父设备方必须有一个相应的公用时隙来接收“Keep-Alives”报文 |
| 管理超帧：入网过程 | 入网请求：从最远端设备开始到网关的路径上，为每个中间设备分配一个链路（不需要提供冗余） |
| | 入网响应：从最远端设备开始到网关的路径上，为每个中间节点分配一个链路（不需要提供冗余） |
| | 为每个设备分配通告报文。通告报文的数量与到网关的跳数成反比 |
| 管理超帧：邻居节点发现 | 邻居节点发现。网络管理器应该为所有的网络设备分配发现链路。邻居节点的发现间隔（DiscoveryInterval）定时器应该被启用来进行邻居节点发现 |
| 管理超帧：网络管理命令 | 与入网请求和入网响应共享等管理链路 |
| 命令请求/响应通信 | 分配共用时隙以满足自组织（Ad-hoc）请求和响应通信 |
| 网关超帧 | 分配给网关超帧的标识符的值应该比较大 |
| | 网关超帧需要设置长度为 40 个时隙。在网关的接入点中，所有时隙都应该被分配 |
| | 调度网关超帧中所有没有分配的时隙，使每个时隙交替地被配置为 XMIT 和 RECEIVE（接收时隙必须是共用的） |
| 特别用途超帧：高吞吐量 | 特别用途超帧是由网关或客户端分配的，以满足资产管理和其他应用程序对高吞吐量的要求。该超帧将被作为“维护”或“块传输”服务类型 |
| 特别用途超帧：维护超帧 | 被分配在手持设备和每个现场设备中。该超帧被用来给现场设备与手持设备之间提供一个高速会话连接。网络管理器将为其每秒钟分配 4 个时隙（每个方向上分配两个链路） |

# 第二部分　WirelessHART 深入

该部分讨论 WirelessHART 标准中的一些关键话题。与 WirelessHART 相关的人士将会对此部分感兴趣。这些话题在几个方面都非常重要。它们将是一些有助于理解 WirelessHART 标准的话题，例如 TDMA 和时隙；它们还涉及一些 WirelessHART 标准中没有描述清楚的话题，例如位顺序和字节顺序；它们还涉及一些 WirelessHART 标准中的兴趣点，例如公共密钥的来源；它们还涉及一些 WirelessHART 产品开发相关的重要话题，例如入网流程；它们也可能是回答一些常见问题的话题，例如安全和共存。

第 7 章涉及 WirelessHART 协议栈相关的话题；

第 8 章涉及 WirelessHART 网络相关的话题；

第 9 章涉及 WirelessHART 标准相关的常见话题；

每章中的每一节阐述一个独特问题，并作为独立单元撰写。读者可按任意顺序阅读各小节，随意选取任何感兴趣的话题。

# 第7章　范　　例

摘要：本章利用一个案例来描述 WirelessHART 网状网络是如何工作的。该案例将涉及无线发射器、执行器和生物反应器。在这个案例中，我们只考虑与传感器相关的无线通信，即在设计和管理这个无线网络的时候我们不考虑使用无线信号来控制执行器。我们将描述如何通过超帧和链路来调度网络通信。我们还将提供两种不同网络拓扑结构下的实验结果，即单跳和多跳网络。在简单的单跳网络案例中，所有的传感器通过 WirelessHART 接入点直接与 WirelessHART 网关相连。而在多跳网络的案例中，多个传感器通过其他的传感器与 WirelessHART 接入点和 WirelessHART 网关相连。

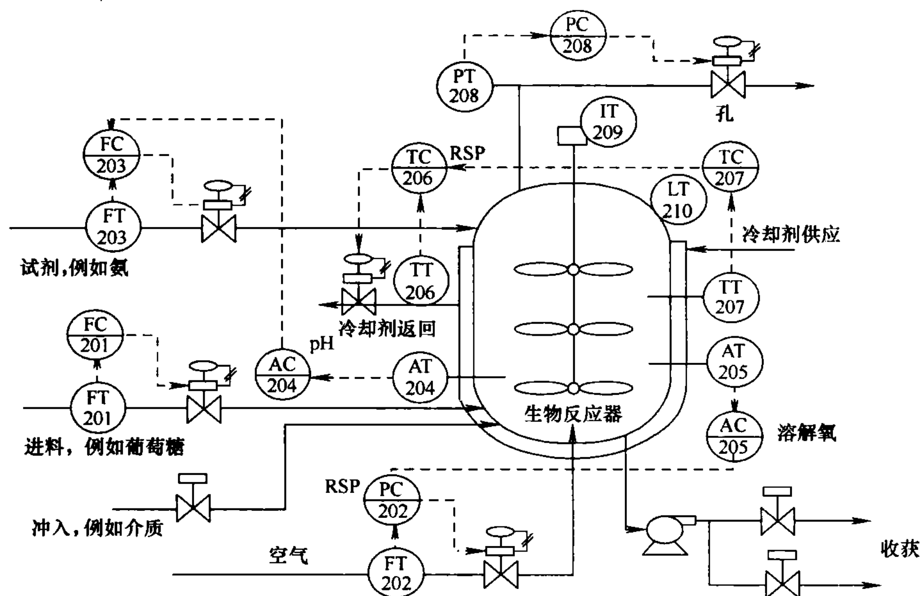



图7-1　生物反应器进程

这个例子是从 HART 7.0 标准中“无线设备规范（HCF_SPEC-290）”的附录 C 中改编而来，并且在论文（Nixon 等，2008）中也有提到。本章所提到的网关即指网关和接入点的组合体。图7-1 给出了生物反应器的结构。该例子涉及的测量仪器、执行器和阀门汇总见表7-1。

表 7-1 生物反应器的仪器和阀门列表

| 分 类 | 设 备 | 测 量 |
|---|---|---|
| 测量仪器 | C1 | 反应器液位（LT210） |
| | C2 | 进料流量（液体 FT201） |
| | C3 | 反应器气压（PT208） |
| | C4 | 反应器温度（TT207） |
| | C5 | 搅拌器放大器（IT209） |
| | C6 | 回水温度（TT206） |
| | C7 | 试剂流（FT203） |
| | C8 | 气流（FT202） |
| | C9 | 溶解氧（AT205） |
| | C10 | pH（AT204） |
| 调节阀 | A1 | 进料流量（FV201） |
| | A2 | 试剂流（FV203） |
| | A3 | 冷却水流量（FV206） |
| | A4 | 泄流量（FV208） |
| | A5 | 气流（FV202） |
| 堵阀 | B1 | 电荷流（FZ211） |
| | B2 | 收获流（FZ212） |
| | B3 | 收获流（FZ213） |

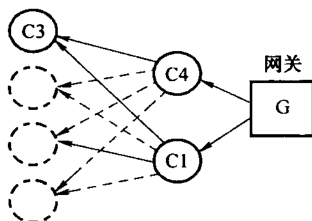
## 7.1 网络管理和上位机请求

WirelessHART 网状网络形成的第一步是为网络管理分配通信资源。希望加入网络的设备首先监听网络中的通告报文，然后利用这个通告报文中的信息产生和发出入网请求。网络管理器在收到该设备发出的入网请求后，将验证该设备的加入密钥以决定是同意还是拒绝这个加入过程。只有这个设备和网络管理器知道这个加入密钥。作为网络形成过程的一部分，网络管理器会通过在管理超帧上创建专用的时隙来实现设备管理和通告功能。对每个新加入的设备，网络管理器将在管理超帧上定义一个时隙用来发送通告报文。与此同时，管理超帧中的一些共享时隙将被预留给新设备，用来与那些发出通告报文的设备通信。这个新时隙的分配信息将被在整个网络内传送，并反馈至所有相关的设备。

新设备都会监听一段时间的通告报文，并据此选择信号最强的一个邻居设备来申请加入网络。在绝大多数情况下，因为一个专用的时隙会被分配用于处理入网请

求，所以新设备可以利用此时隙发送入网请求给网络管理器。然而，如果两个新设备碰巧在一个相同的时隙上用相同的信道发送入网请求，那么入网请求报文就会彼此间发生冲突。这时，设备可以检测到这种冲突，并退避一段时间后再尝试发送。这样，不同的入网请求就会被分隔一段时间，那么下一次尝试发送时成功的可能性就大大地增加了。

网络设备应该逐个地加入网络。网络管理器根据它们之间的信号强度来决定整个网络的路由路径。信号强度主要由工厂的物理布局、网络跳数和数据流量等决定。整个网络的路由路径还会被进一步调整以发送网络诊断信息和重传等。在调度网络管理通信的时候，我们可以假设在同一个时间上只允许发生一个网络管理通信。这样，当一个设备有多个目标设备时，它们之间的通信可以被调度在同一个时隙上发生，从而可以减少调度时所需的时隙数和能耗。对于响应通信的调度，我们需要考虑网络设备的最大响应时间，即网络设备从收到命令到作出响应的时间。例如，假设网络设备的最大响应时间是0.5s，当4个设备加入网络时，我们会创建两




| 设备 | 对端设备 |
|---|---|
| C3 | C4,C1 |
| C4 | G |
| C1 | G |

网络管理-发送帧/图

| 信道偏移 | 时隙0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | | *n* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | G广播 | G=>* | | | | G=>C4 | C4=>C3 | | | | | |
| 1 | C4广播 | C4=>* | | | | G=>C1 | C1=>C3 | | | | | |
| 2 | C1广播 | C1=>* | | | | | | | | | | |
| 3 | C3广播 | C3=>* | | | | | | | | | | |

网络管理-接收帧/图

| 信道偏移 | 时隙0 | 1 | 2 | 3 | | 55 | 56 | 57 | 58 | 59 | | *n* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | | | *=>G | | C3=>C1 | C4=>G | | | | | |
| 1 | | | | *=>C4 | | C3=>C1 | | C1=>G | | | | |
| 2 | | | | *=>C1 | | | | | | | | |
| 3 | | | | *=>C3 | | | | | | | | |

图7-2　网络管理帧

* —临时的时隙，保留用于与新设备的通信

个如图 7-2 所示的管理超帧。为简单起见，我们把 WirelessHART 网关和 WirelessHART 接入点放在一起标记为“G”。

在超帧中，只有与每个设备直接相关的部分会被发送给这个设备。图 7-3 给出了在这个例子中与设备 C4 相关的超帧。

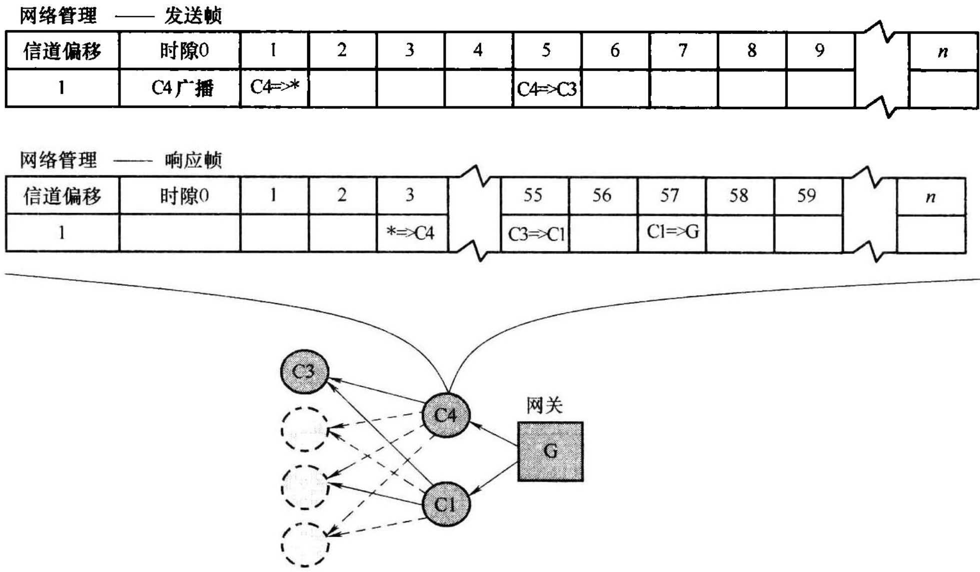



图 7-3 C4 中的网络管理帧和图

* —临时的时隙，保留用于与新设备的通信

网络管理请求和响应的速度主要取决于设备和网络管理器之间的通信频率。在这个例子里，网络管理请求的频率可以通过调整超帧的长度来决定。例如，如果超帧的长度是 100 个时隙（一个时隙是 10ms），那么一次请求和响应再加上一次重传的最快传送速率是每秒钟一次。如果某个超帧的时隙与网络管理超帧的时隙相冲突，那么该超帧对应的网络通信就将会被自动推迟以避免冲突，这是因为网络管理超帧拥有更高的优先级。

## 7.2 过程测量

大多数现场设备主要用于过程测量。过程自动化上位机对采样频率的要求主要取决于过程设备和具体的测量类型，例如压力、温度、流量、液位和分析结果。所以，作为过程自动化上位机配置的一部分，用户需要对网络设备配置以下信息：

1）与设备一一对应的设备标签，例如 HART 标签。

2）网络设备可以获得的测量值。

3）每个测量值被传送到网关的频率。

生物反应器案例中的现场设备可以按照表7-2来设置测量和更新频率。

表7-2 生物反应器的测量和更新频率

| 设 备 | 测 量 | 更新频率 |
|---|---|---|
| C1 | 反应器液位（LT210） | 16s |
| C2 | 进料流量（液体-FT201） | 1s |
| C3 | 反应器气压（PT208） | 1s |
| C4 | 反应器温度（TT207） | 4s |
| C5 | 搅拌器放大器（IT209） | 8s |
| C6 | 回水温度（TT206） | 16s |
| C7 | 试剂流（FT203） | 1s |
| C8 | 气流（FT202） | 1s |
| C9 | 溶解氧（AT205） | 4s |
| C10 | pH（AT204） | 4s |

为了能够为不同的过程数据采样率配置不同的超帧，现场设备的采样率需要被设置成其能够支持的最快采样率的整数倍。在本案例中，设备支持的采样率被定义为$2x$，这里$x$是非负的整数值，例如采样率可以选择为1 s、2 s、4 s、8 s、16 s和32 s。

如图7-4所示，为了避免传送到网关的测量值有延迟，传感器的测量过程与测量值的传送之间的协调是很重要。

在WirelessHART网络中，与过程测量相关的通信调度可以通过两个方法来简化。第一种方法是为每个采样频率定义一个超帧；第二种方法是根据采样频率从快到慢地为传送测量数据分配时隙。在产生的调度中，一个设备在一个时隙上只能出现一次，这是因为在某个给定时间内设备在某个信道上只能接收或者发送数据。

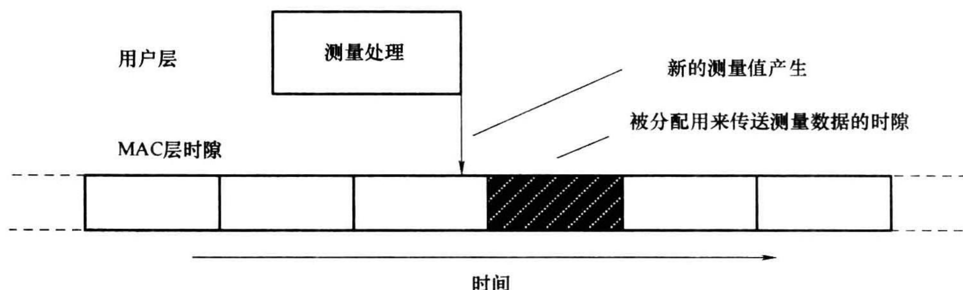



图7-4 同步测量处理和传输

## 7.3　调度范例——单跳网络

我们根据以上推荐的方法为每个采样频率定义一个超帧并且按照采样的快慢来分配时隙。假设所有的测量设备都通过一跳连接到网关，那么生物反应器对应的网络拓扑图将如图 7-5 所示。图 7-6 给出了在这种网络配置下的通信调度。

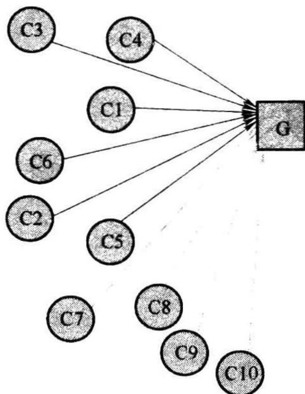



图 7-5　生物反应器范例——单跳网络

帧 0 —— 1 s的更新率

| 信道偏移 | 时隙 0 | 1 | 2 | 3 | … | 99 |
|---|---|---|---|---|---|---|
| 0 | C2=>G | C3=>G | | | | |
| | | | | | | |

帧 1 —— 4 s的更新率

| 信道偏移 | 时隙 0 | 1 | 2 | 3 | 4 | … | 399 |
|---|---|---|---|---|---|---|---|
| 0 | | | C4=>G | | | | |
| | | | | | | | |

帧 2 —— 8 s的更新率

| 信道偏移 | 时隙 0 | 1 | 2 | 3 | 4 | 5 | 6 | … | 799 |
|---|---|---|---|---|---|---|---|---|---|
| 0 | | | | C5=>G | | | | | |
| | | | | | | | | | |

帧 3 —— 16 s的更新率

| 信道偏移 | 时隙 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | … | 1599 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | | | | C1=>G | C6=>G | | | | | |
| | | | | | | | | | | | |

图 7-6　不同的帧对应不用的采样频率——单跳

当某个设备到网关的传输失败后，在通信调度时，额外的时隙可以被安排在紧随传输时隙之后以支持立即重传（如果需要的话）。

## 7.4　调度范例——多跳网络

前一个例子是基于最理想情况的，即所有网络设备都能通过一跳与网关通信。然而，在很多情况下，设备需要通过多跳才能与网关通信。

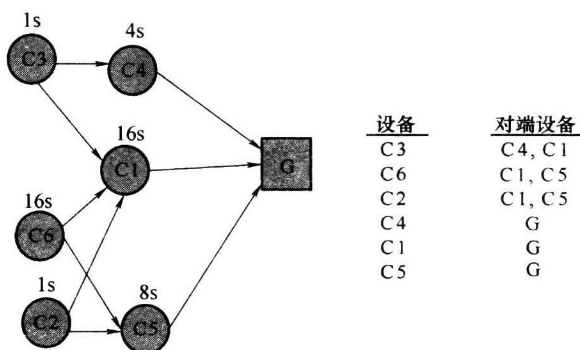



图 7-7　生物反应器范例——多跳网络

WirelessHART 网络是通过网络设备的不断加入而逐步形成的。当某个网络设备不能和网关直接通信时，我们必须分配对应的时隙来为其路由数据。另一方面，如果某个网络设备被配置成允许拥有多个对端设备，那么我们必须分配对应的时隙来与每个对端设备通信。当为两个对端设备都分配了时隙后，超帧上对应于第二个设备的时隙只有当第一个时隙上的通信失败时才会被使用到。图 7-7 显示了路由和支持多个对端设备对通信调度的影响。由此产生的通信调度如图 7-8 所示。我们可以看到设备 C3 和网关之间的数据传输延迟在 30ms（没有重传）到 60ms（多次重传）的范围内。相比于 1s 的采样频率，这个数据传输延迟以及随之产生的抖动都是很小的。

用于重传的时隙需要被提前分配好以提高传输的可靠性。当不需要重传的时候，这些额外的时隙分配会降低网络的带宽。WirelessHART 提供了其他的方式对此进行补偿。例如，WirelessHART 允许最多同时使用 15 个信道，这样就可以把网络通信的带宽增加 15 倍。WirelessHART 的有效带宽高于传统 HART 的有效带宽。

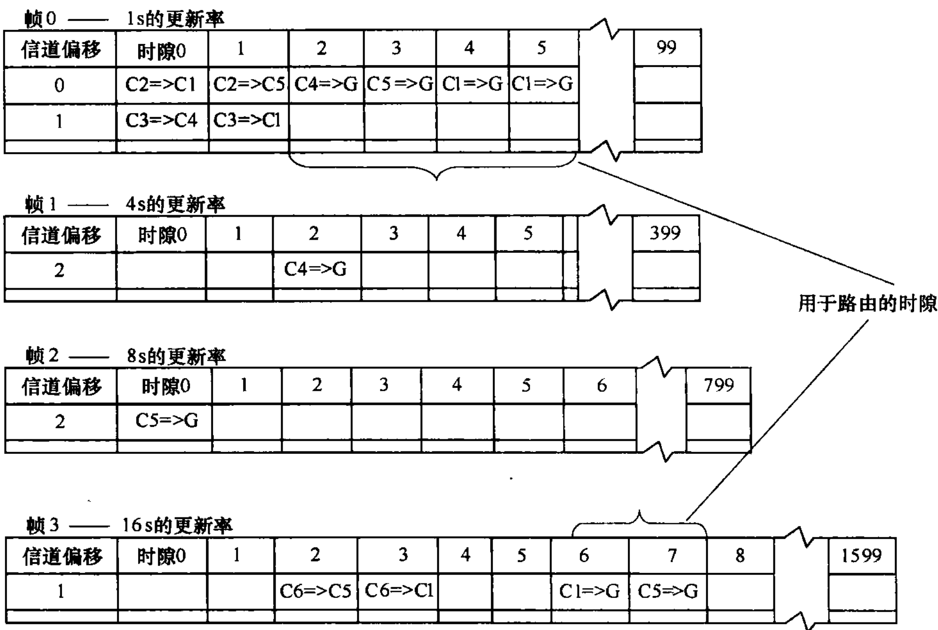



图7-8　不同的帧对应不用的采样频率——多跳

# 第 8 章　WirelessHART 协议栈剖析

摘要：在这一章中，我们将深入探究一些精心挑选的、与 WirelessHART 协议栈相关的话题。这些话题被归纳成以下几类：物理层、网络层、应用层、跨层和其他。这些话题像章节标题一样被列出。

## 8.1　物理层

### 8.1.1　物理信道和最大带宽

IEEE 802.15.4 标准在 2.4GHz 频段定义了 16 个信道，而 WirelessHART 标准当前只使用其中的 15 个信道。许多基于 IEEE 802.15.4 标准的网络在运行期间只使用一个信道，但是 WirelessHART 网络能使用所有 15 个信道（信道 26 的频段在某些地区是被禁止的，因此决定排除使用该信道）。此外，WirelessHART 标准允许同时占用多个信道。换句话说，同一网络中的 15 对设备能在同一个时隙、在 15 个不同信道中同时进行着 15 对通信。

现在，我们来分析 WirelessHART 网络的最大可用带宽。IEEE 802.15.4 标准定义其最大原始数据率为 250kbit/s，其最大报文长度（例如物理层有效载荷）为 127B。在 WirelessHART 标准中，10ms 的时隙能传输至多一个数据报文[⊖]。因此，WirelessHART 网络中每个信道的最大数据率是 127B/10ms，即 12.7KB/s。由于 15 个信道，因此 WirelessHART 网络的可用总带宽为 190.5KB/s，这也是 WirelessHART 网络内能同时存在的最大数据率。如果一个 WirelessHART 网络有 15 个 WirelessHART 接入点，那么 WirelessHART 网络与外界的可用带宽也就是 190.5 KB/s。

在过程控制中，过程和控制数据通常用一个专门的数据报并在一个专用链路上传输。因此，最大可用数据率是每秒 15 个数据报，或者每秒 1500 个数据报。每个数据报通常包括 1 ~8 个设备测量值、状态和单位信息，并被命令 9（Command 9）发布。大多数设备将包含 2 ~4 个 4B 的浮点值，这样一个命令 9（Command 9）数据报的有效载荷为 21 ~37B，因此实时测量数据的最大可用吞吐量为 31.5 ~55.5KB/s

⊖ 确认报文不属于数据报文。——译者注。

$(15\times100\times21\sim15\times100\times37)$。

如果两对通信彼此间不相互干扰，那么它们有可能同时使用同一信道。但是，此处并没有考虑该种情况，因为典型的 WirelessHART 网络通常是小型网络。

### 8.1.2　包长度与可靠性

这里有一个争论，即短的数据报可以获得可靠传输。其理由是越短的数据报所需要的发送时间越短，因此被噪声干扰的机会越小。另一方面，将几个命令汇合成一个更长的数据报以增强吞吐量的方式更可取。同时，为了提高可靠性而单独地发送短数据报将会使每个数据报都暴露在干扰中。因此，WirelessHART 标准采纳了后一种方式，即将几个短命令汇合成一个长数据报。

事实上，包长度对噪声环境中的可靠性贡献较少。IEEE 802.1.4-2003 标准的附录 E 提供了由信噪比引起的位误码率（Bit Error Rate，BER）公式：

$$BER=\frac{8}{15}\times\frac{1}{16}\times\sum_{k=2}^{16}-1^{k}\binom{16}{k}e^{\left(20\times SINR\times\left(\frac{1}{k}-1\right)\right)} \tag{8-1}$$

IEEE 802.1.4-2003 标准附录 E 中的图 E.2 描绘了该公式的曲线。当信噪比为 2dB 时，位误码率（BER）小于 0.000001。对于一个 127B 的最长包，每 1000 个包大约有一个位错误。数据报大小的少许不同对丢失率不会有太大影响。

突发的干扰比持续的背景干扰更容易造成包丢失。即使最长报文的长度对于位误码率的计算而言仍然是很小的。

### 8.1.3　跳信道

用于通信的物理信道是通过如下的方法计算得出的：选用的物理信道号被存储在一个数组里，每当针对某个链路的时隙被确定时，那么该链路的信道号就可被计算出。绝对时隙数（Absolut Slot Number，ASN）与链路的偏移量之和除以该数组的长度，其余数即为该链路对应的信道号在该数组中的索引值。因为绝对时隙数是单调累加的，任何选用的物理信道理论上都能在某时被选取到。然而，确保尽可能随意的跳信道是必须被考虑到的。

例如，假设所有 15 个信道都可用、超帧长度为 15、超帧中的第一个链路是偏移量为 0 的标准链路，那么第一个物理信道将会被一直分配给这个链路。然而，如果我们将超帧长度改变为 16，信道数仍然为 15，那么第一个物理信道在第 1 次超帧中被分配给该链路，第二个物理信道在第 2 次超帧中被分配给该链路，直到所有 15 个物理信道被分配给第 15 次超帧。

活跃信道数组没有必要包含所有的物理信道。因为某些信道可能被列入黑名单了，所以数组索引号没有必要等于物理信道序列号。

链路被定义在一个超帧里。链路的 ASN 的值等于超帧大小的倍数加上超帧内

链路的偏移量。如上例，如果超帧大小是活跃信道数的倍数，那么链路将一直使用同一个物理信道。这种情况应该尽量被避免，特别是对于通告报文而言，因为我们希望在所有活跃信道上发布通告报文。超帧长度的不同设置将会导致某个链路只会使用到“选用的信道”的一个子集。理想情况下，超帧长度应该与“选用的信道”数互素，这样某个链路就能使用到所有的“选用的信道”。

### 8.1.4 健康报告

设备与邻居设备间的通信能力是形成和梳理 WirelessHART 网状网络的一个关键尺度。所以，设备的每个邻居表实体中都维护有一些统计信息，其中包括平均接收信号水平（Received Signal Level，RSL）、发送和接收数据报的统计信息、与邻居设备最后一次通信的时间戳。对于互联的邻居设备，RSL 遵照以下公式使用 IIR 滤波器计算出：

$$RSL = RSL - (RSL / RSLDamp) + (MeasuredRSL / RSLDamp)$$

式中，MeasuredRSL 是当前数据报的 RSL；RSLDamp 是衰减因子，RSLDamp 必须是 2 的指数，其默认值为 64。

设备与某个已发现的邻居设备（例如还没有通信的邻居设备）之间可能有多次 RSL 值，设备会从这些 RSL 值中选出最大值并返回给网络管理器。同时，在选取 RSL 值的过程中，设备也应当尽量考虑选取最新的 RSL 值。

设备周期性地将其邻居节点的健康报告发送给网络管理器。健康值主要是其邻居设备的 RSL 值。每当 RSL 值被发送后，该值就会被清零。这对于网络管理器优化网络配置很重要。每次最多报告四个邻居设备的健康报告，然而网络管理器也可以要求更多的健康报告。

两种命令（命令 780 和命令 787）可用来报告邻居设备健康信息。设备必须周期性地使用这两种命令来报告邻居设备的健康信息。这两种命令被用来报告不同的信息。命令 780 提供了相连邻居设备的统计信息，例如分配给该邻居设备的链路。命令 780 还可以报告其他信息，如通信统计信息。命令 787 仅提供已发现（但还没连接）的邻居设备的信号强度。当设备在一个发现链路中侦听到通信时，这意味着该设备可能发现了某个邻居设备。新设备能通过捕获邻居设备发出的通告报文从而发现这些邻居设备。实际上，新设备发出的入网请求报文必须包括命令 787。如必要的话，在普通链路被配置前，新设备在入网链路中同时还需要发送 Keep-Alive 报文以保持时间同步和收集健康信息。

网络管理器可以利用不可用信道信息来产生信道黑名单。但是，目前 WirelessHART 标准还没有提供一种机制，来让设备报告不可用的物理信道。因为信道黑名单被用于跳信道的计算，所以在网络正在运行的时候改变信道黑名单是一个巨大的挑战。此外，WirelessHART 标准被设计成能容忍坏的物理信道。

## 8.2 数据链路层

### 8.2.1 时隙

WirelessHART 网络中的通信时隙长度为 10ms。请参考第 3 章中图 3-4 和表 3-2 中定义的标志。设备准确地解析和实现这些规定的时间点对于通信和同步来说很重要。

(1) 源设备　发送方首先等待 TsCCAOffset 时间段，然后在 TsCCA 时间段内持续检查信道是否空闲。如果信道是忙的，那么发送方在该时隙内将不做任何事情直到下一个时隙。如果信道是空闲的，发送方将在 TsRxTx 时间段内切换到发送模式，然后发送出整个数据报。当数据报发送完毕后，发送方等待 TsRxAckDelay 时间段，然后开始侦听确认包。如果发送方在 TsAckWait 时间段内都没有收到确认包，那么发送方将会认为此次发送失败了并采取相应的行动。否则，发送方将会接收并处理确认包。确认包包括接收状态和一个时间调整值。如果接收方不是发送方的时钟源，那么时间调整值将会被忽略掉。如果接收方是发送方的时钟源，那么发送方将用这个时间调整值来调整其时钟，从而实现与接收方的时间同步。这样，发送方在下一个时隙就将与接收方同时开始。

(2) 目标设备　接收方首先等待 TsRxOffset 时间段，然后在指定的信道上开始侦听数据报。如果在 TsRxWait 时间段内没有数据报到达，那么接收方将会认为该时隙没有被使用，同时等待下个时隙的到来。如果在 TsRxWait 时间段内有数据报到达，那么发送方发出的数据报将会被接收并处理。然后，接收方在 TsTxAckDelay 时间段内准备好确认包，并随后发出该确认包。如果发送方是接收方的时钟源，接收方将基于数据报期望到达时间值与实际到达时间值的差额来调整其时钟，并设置下一个时隙的开始时间以实现与发送方同步。

针对时隙图的解释是非常复杂的。这里对此提出一些建议：

1) 整个数据报依次包括四个字节的前同步码、一个字节的 SFD、一个字节的物理层帧头及物理层载荷。物理层帧头中含有物理层载荷长度的信息。前同步码的开始发送即可被认为是数据报的开始。在前同步码开始的时候，由于数据报的信息还并没有被提供，所以接收方不得不等候片刻以确定正在到达的数据报是合法的或者只是一些噪声信号。对于许多硬件平台，第一个中断直到获得了数据报长度时才会产生，例如物理层帧头被接收到时。因此，在具体实现的时候，侦听超时值应该加上用于接收物理层帧头的额外时间。

2) 在 WirelessHART 标准中，网络管理器能向某个设备发送命令 805，使其不执行信道空闲评估（CCA）。这时，发送方还是应该在 TsTxOffset 时间段之后开始

发送数据。接收方在发出确认包之前不执行信道空闲评估（CCA）。

3）信道空闲评估（CCA）用于检测来自于网络外的干扰。如果两个设备共享一个链路且都想发送数据，那么它们将完成信道空闲评估后开始各自发送数据报，这两个数据报可能会相互干扰。接收方都无法得到各自的数据报，也无法发出确认数据报。假如这样的话，这两个发送方都会发送失败。事实上，由于这两个发送方彼此间很难完全同步，所以上述情况是非常罕见。因为这两个设备没有完全同步，所以较慢的发送方将会由于信道空闲评估而放弃该链路，较快的发送方将会先抢到信道从而能成功地发送自己的数据报。

4）如果接收方不是时钟源，那么其确认数据报中的时间调整值将不会被使用到。即便如此，接收方仍然必须遵照 WirelessHART 标准而发送出时间调整值（TsError）。

5）TsRxTx 是射频从发送模式切换到接收模式的时间，或者是从接收模式切换到发送模式的时间。WirelessHART 规定的 TsRxTx 值与 IEEE 802.15.4 标准定义的一致。市场上大部分硬件芯片的切换时间都小于该值，但是每个具体实现都必须满足 WirelessHART 规定的这个时间值。这样，设备如何实现 WirelessHART 规定的 TsRxTx 值由设备自己决定。WirelessHART 标准所关心的是在恰当时间发送出数据报。

6）数据报文发送结束后，接收方在 TsTxAckDelay 之后应该立即发送确认报文。图 3-4 容易让人误以为：确认报文应该在数据报文发送开始后的某个固定时间发出。

7）如果接收方是时钟源，那么接收方必须在发送方期望的时间而不是正确地时间发出确认报文。这样，我们会有更好的通信成功率。

8）在 WirelessHART 标准中，TsAck 值为 832ms 是由于要发送 26 个字节，整个确认报文的长度为 26 个字节。在入网期间，新设备将会使用 8 个字节的长地址。长地址比短地址多 6 个字节。所以如果新设备使用了长地址，那么 TsAck 值将会变成 1024ms。

9）用于加密确认报文的密钥应该采用用于加密数据报文的密钥，该密钥可能是网络密钥也可能是公共密钥。已接收数据报中的密钥位表明用的是哪个密钥。

10）WirelessHART 标准中的两个术语（TsTxWait 和 TsRxWait）的含义相同。

11）WirelessHART 协议栈的实现应该力求满足时隙中规定的精确时间点。如果协议栈能在 ±100ms 的偏差范围内完成一些行为（如发送、开始等待、停止等待等），那么它将被认为满足了 WirelessHART 标准要求。例如，如果某个设备能在接收数据报文结束后 900 ~ 1100ms 间确认该数据报文，那么该设备是符合 WirelessHART 标准的。在接收数据报结束报文，如果设备在 899ms 前或 1101ms 后确认该数据报文，那么该设备是不符合 WirelessHART 标准的且不能被认证通过。

### 8.2.2 链路

链路定义了某个时隙中的通信类型。链路共有四种类型，分别是普通链路、广播链路、加入链路和发现链路。

（1）普通链路　普通链路是最常见的链路。它有源地址和目标地址。源设备可以使用普通链路来发送一个数据报文给目标设备。

（2）广播链路　广播链路与链路的发送方相关。发送方使用广播链路发出无需确认的广播报文。广播报文中的目标地址都为 0xFFFF。

（3）加入链路　加入链路也必须与设备有关。该设备既可以是源设备也可以是目标设备。换句话说，该设备既可在加入链路中处于发送状态，也可以在加入链路中处于接收状态。加入链路中的这两种状态被广播在通告报文中。网络设备发出的通告报文包含了足够信息以使得新设备能通过自己加入网络。新设备能从通告报文中解析出足够的信息，然后利用这些信息完成加入网络的过程。

（4）发现链路　发现链路是一种用于维护设备间互联的特殊链路。发现链路的主要作用是允许设备发现其周围的邻居设备。在一个随机时间后，设备将使用一个发现链路向其最长时间没有通信的邻居设备发送一个 Keep-Alive 报文。如果发现链路与其他链路同时都想占用某个时隙，那么发现链路要让其他链路优先使用该时隙。如果没有数据要发送，设备将在发现链路时侦听信道。如果 Keep-Alive 报文不是发送给自己的，那么该设备将持续侦听以便记录正与其会话的邻居设备的通信状态。

在 WirelessHART 标准中，链路（Link）被用于描述两个邻居设备间的 MAC 层连接。连接（Connection）被用于描述两个设备间的网络层连接，这两个设备能通过中间节点而相互通信。

链路可能会被多个发送方共享和竞争，通常会导致通信的冲突。这时，退避机制可被用来解决这种冲突。在共享的普通链路中，只能有一个接收方，但可以有多个发送方。加入链路可被共享给多个入网设备，以便它们能通过竞争的方式来与代理设备通信。发现链路是共享的，设备可以通过竞争的方式占有发现链路来发送或侦听数据。

链路能被加入到一个活跃的超帧。但是，一个已经存在的链路只能被从一个非活跃超帧中移除。除了先被移除后再被加回去这种方式以外，链路不能通过其他的方式更新。

### 8.2.3 同步

WirelessHART 网络设备中的时钟可能会慢慢漂移，所以两个网络设备间必须不断地调整它们的时钟以保持完全同步。依据 WirelessHART 标准，任何一次时隙

通信即可完成一次时间同步。在一次时隙通信内，接收方将在发送方的数据报文到达时打下时间戳，并将该时间戳与期望到达的时间相比较。设备可依据 WirelessHART 标准规定的时隙时间点和自身的时钟计算出期望报文到达的时间。偏差量 TsError 是两个设备间的时钟偏差，它通常以毫秒（ms）为单位。如果发送方发出的数据报文比接收方期望的时间早到达，那么 TsError 为正值；否则，TsError 为负值。如果发送方是接收方的时钟源，那么接收方会将其自身时钟减去 TsError。

TsError 也会被编码成确认报文中的两个字节。由于发送方的数据报文必须发送在接收方的侦听窗口内，因此 TsError 受侦听窗口大小的限制。两个字节足够用来编码最大允许偏差。如果 TsError 为非负，那么这两个字节将会是表达 TsError 的非负整数；否则，这两个字节将会是取值为 0xFFFF-|TsError|的非负整数。如果接收方是发送方的时钟源，那么发送方将会从确认报文中取出 TsError 值，并依据此值调整自己的时钟。

WirelessHART 网关是整个 WirelessHART 系统的根时钟源，而 WirelessHART 接入点是所有进行无线通信的节点的根时钟源。如果 WirelessHART 网络中有多个 WirelessHART 接入点（AP），那么这些 WirelessHART AP 之间也必须相互时间同步。WirelessHART 标准并没有定义网关与 AP 之间的时间同步方法。如果多个 WirelessHART AP 之间要通过 WirelessHART 网络来实现时间同步，那么其中一个 AP 应该为主时钟源，而其他 AP 应该像网络设备一样与其同步。假如多个 WirelessHART AP 被放置在网络的不同地方以提高网络吞吐量，那么它们之间可能无法直接通信。这时，这些接入点仍需要与网关同步，它们可以通过与网络设备时间同步从而实现与网关的时间同步。

### 8.2.4 Keep-Alive 间隔时间

两个相邻设备可以利用每次通信来实现时间同步。如果它们在一段时间内没有需要交互的信息，那么它们应该交互 Keep-Alive 报文以保持彼此间的时间同步。根据 WirelessHART 标准规定："当温度变化少于每分钟 2℃时，设备应该在 30s 内请求发送一次 Keep-Alive 报文。这大概相当于一个精度小于 $10 \times 10^{-6}$ 的温度补偿晶振。"

在这一小节，我们将关注两个设备间如何维持时间同步。在 WirelessHART 网络中，两个设备只要能周期性地完成时隙通信，那么就能实现时间同步。

一个 WirelessHART 报文起始于一个 128μs 的前同步码，接着是 32μs 的 SFD 字段，最后跟随的是数据报。在前同步码之前，我们需要额外的时间用于信道空闲评估（CCA）。对于相互通信的两个设备，接收方必须在发送方发出前同步码之前开始侦听（案例 A，见图 8-1）；此外，在接收方停止侦听之前，发送方的物理层帧头必须已经发出（案例 B，见图 8-1）。假设 $\gamma$ 是两个设备间时隙开始的时间偏差，

我们就有以下两个相关的公式：

$$y + TsRxOffset \leqslant TsTxOffset \tag{8-2}$$

$$y + TsTxOffset + tHead \leqslant TsRxOffset + TsRxWait \tag{8-3}$$

图 8-1 描述了两个计算 Keep-Alive 时间间隔的案例。同时，也请参照图 3-4。

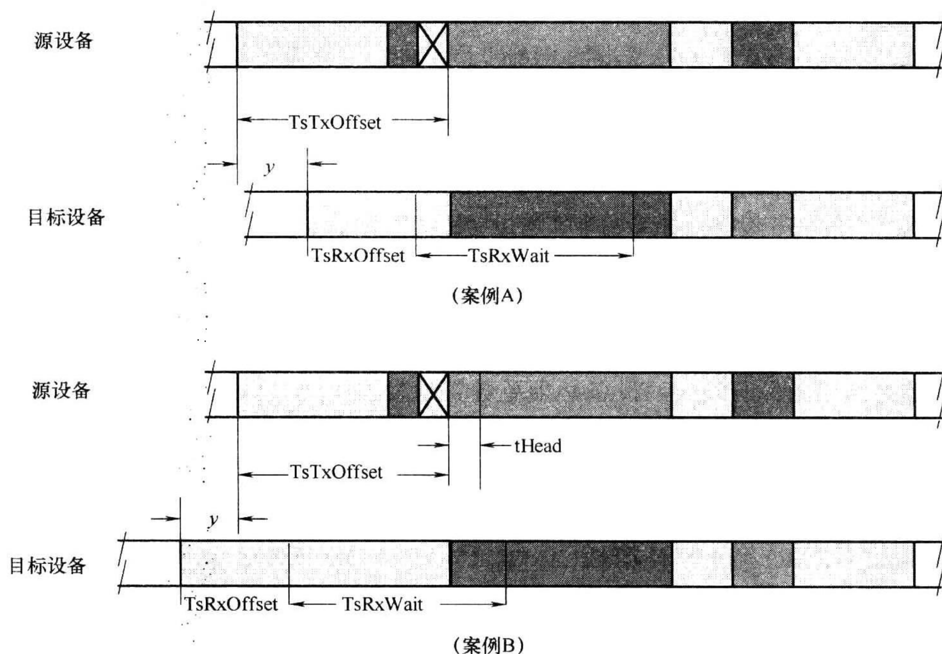



图 8-1　计算 Keep-Alive 时间间隔

使用表 8-1 中的默认值，我们可以得出 $y \leqslant 100\mu s$。

表 8-1　IEEE 802.15.4 在 2.4GHz 频段的时间值和详述（摘录）

| 字　符 | 值 |
|---|---|
| tHead（preamble + SFD + PHR） | 192μs |
| TsTxOffset | （2120 ± 100）μs |
| TsRxOffset | （1120 ± 100）μs |
| TsRxWait | （2200 ± 100）μs |

假设所有 WirelessHART 网络设备的时钟精度为 $x \times 10^{-6}$。即时钟每秒钟偏移 $x\mu s$。因为两个设备的时钟可能向两个相反的方向偏移，所以这两个设备需要每隔 $y/2x$s 同步一次。因此，当时网络设备的时钟精度都为 $10 \times 10^{-6}$时，Keep-Alive 时间间隔为 50s。WirelessHART 标准规定了时隙内多种时间常量的偏差为 ±100μs，

这是为了容许设备在软件和硬件方面的不精确实现（例如，即使接收方的时钟非常精确，并且它被编程为在报文接收完毕后 1μs 发出确认报文，但是确认报文的实际发送时间可能并不是报文接收完毕后 1μs）。因为 WirelessHART 标准允许 ±100μs的时间偏差，所以上述的 $y$ 应该再减去 200μs，因此 Keep-Alive 的时间间隔应该为 40s。

事情在此并没结束。在 WirelessHART 网络中，网络设备与根时钟源可能相隔几跳。依据 WirelessHART 标准，网络管理器可以将某个网络设备配置成是否是其他网络设备的时钟源。整个 WirelessHART 网络的时钟源被配置成了一个非闭环的方向图。在该方向图中，某个设备的进入边的源头是该设备的时钟源。根时钟源至少有一条路径到网络中的任一设备。如果两个邻居设备距离时钟源 $z$ 跳远，在最坏情况下这两个设备应该每隔 $y/(x\ (z+1))$ s 交换一次 Keep-Alive 报文。为了保持全网同步，网络管理器必须非常小心地分配时钟源和每个设备的 Keep-Alive 时间间隔。

入网设备在被完全配置之前可以利用加入链路发送 Keep-Alive 报文。因为加入链路是共用的，所以入网设备必须更频繁地发送 Keep-Alive 报文以防止冲突引起的发送失败。网络管理器也必须提供足够的加入链路，或者足够快地分配普通链路给新设备使用。如果入网设备要发送 Keep-Alive 报文，它可能不得不使用公共密钥。代理设备应该能够响应入网设备发出的 Keep-Alive 报文。

WirelessHART 物理层使用 IEEE 802.15.4 2.4GHz 频段的物理层，其符号率为 62.5 千字符/秒（ksym/s）（偏差为 $\pm 10^{-6}$）。如果我们使用 IEEE 802.15.4 兼容的硬件平台，那么我们可能不得不接受规定的 $40\times10^{-6}$偏差。确认报文的时机是基于发送方的时间，例如总是在发送报文结束后 1ms。时钟偏移在 1ms 内差不多为 $0.002x$μs。就通信而言，这不是一个要素。

WirelessHART 网络设备的时钟可能是同向的偏移，也可能由于老化或温度而随机地偏移。标准晶振（如 Maxim™公司的 DS32kHz）在温度范围 0～40℃时偏移为 $\pm2\times10^{6}$，在温度范围 -40～85℃时偏移为 $\pm7.5\times10^{-6}$。为了将偏移控制在要求的范围内，WirelessHART 网络设备必须使用一些老化补偿或温度补偿机制。以上的计算是考虑的最坏情况。在很多情况下，即使两个设备的实际时间同步偏差大于计算出的时间偏差，这两个设备仍有可能可以相互通信。

### 8.2.5　时钟偏移和精度

时钟偏移通常有两种形式：一种偏移是时钟频率稍微大于或小于标准频率，对于这种情况，我们能够通过周期性地加上或减去一些时钟脉冲来补偿，从而使时钟以准确的速率运行；另一种偏移是时钟频率时快时慢，对于这种情况，我们只能让设备不断地与其时钟源同步。

### 8.2.6 广播报文

如果我们定义广播为一个发送方向多个接收方发送数据，那么 WirelessHART 标准定义了几种不同类型的广播。

（1）通告 通告报文能在发送链路、普通链路、广播链路、入网链路或发现链路中被传送。每当链路可用的时候，通告报文即可被传送出。通过利用所有可能的链路，我们能使新设备快速地获得入网信息并加入网络。网络管理器也能设置发送通告报文的时间间隔或终止通告。

2.4GHz 频段的 16 个信道用两个字节即可代表，但是通告报文载荷中的信道位图并没有被限制为两个字节，这是因为 WirelessHART 以后的版本将可能支持更多其他频段的信道。

（2）广播 WirelessHART 广播报文非常接近于广播的定义。通常，发送方使用的广播地址为 0xFFFF，所有配置了广播接收链路的设备都将侦听该广播报文。在 WirelessHART 标准中，设备被允许利用广播链路来向某个邻居设备发送数据报文。这时，指定的接收设备将会响应该数据报文，而所有其他处于侦听的邻居设备仅需简单地丢弃该数据报文。

（3）发现 发现链路能被任何设备使用来向目标设备发送 Keep-Alive 报文。目标设备将告知已收到 Keep-Alive 报文，而其他设备也将侦听该报文以更新其邻居健康信息。

## 8.3 网络层和传输层

ISO 网络模型中，传输层通常负责大块数据报的分解和重新组装。然而，WirelessHART 标准采用一种独特的方式来处理大块数据。该种方式在规范 190 中被定义，即“块数据传输规范（Block Data Transfer Specification）”。传输层头部的长度仅为 1B。该字节包括了 1bit 的确认标志位、1bit 的响应标志位、1bit 的广播标志位和 5bit 的序列号。因为传输层被简化了，为了方便，传输层被详述在网络层文档中。

### 8.3.1 会话和传输表：谁拥有谁

ISO 协议模型将会话层至于传输层之上，传输层置于网络层之上，网络会话管理着传输表。换句话说，会话拥有传输表。然而，WirelessHART 标准没有定义会话层，会话被定义在传输层之下的网络层里。当读到“WirelessHART 网络管理规范”[⊖]中类似图 33 的地方时，读者需要意识到 WirelessHART 会话被定义在网络

⊖ 相关规范名称和编号见参考文献，读者可自行查找。——译者注

层里。

虽然网络管理器能在现场设备之间建立起点对点的会话和路由，但是这并不是非常常见的情况。大多数情况下，路由是建立于网络管理器或 WirelessHART 网关与现场设备之间的。当设备间点对点通信被使用的时候，一个设备将发布报文，而另一个设备将缓存这个突发的报文。但是，手持设备是一个例外。手持设备与网络设备间需要建立起点对点的会话。

## 8.3.2 安全层

WirelessHART 标准在网络层既使用加密技术来加密网络层载荷，又利用 4B 的消息完整性代码（MIC）来实现认证。这样，网络层和传输层之间在逻辑上存在着一个简单的安全层。从协议栈层次来说，该安全层位于传输层之下，所以传输层的包被作为安全层的载荷而被加密。该安全层的头部包含有 1B 的控制字段、1B 或 4B 的随机数（nonce）计数器字段、4B 的消息完整性代码（MIC）。

## 8.3.3 广播和响应

在 WirelessHART 网络中，广播报文能被传送至所有的网络设备。广播报文的使用既能减少网络资源的负担，又能节省网络设备的能耗。网络密钥的更新就是利用广播报文来实现的。然而，数据链路层层面的广播链路不支持确认。因此，网络管理器需要确保所有设备已经收到命令并正确地响应。广播设备发出一个广播报文，通常将会接收到多个响应报文。如果某个设备接收到该广播报文但是没有给出响应，那么广播设备将会重传该广播报文或者针对该设备发出一个需要确认的单播报文。对于改变网络密钥而言，这一点是非常重要的；否则如果网络设备错过了请求改变网络密钥的广播报文，那么它将失去同步。此外，广播报文以广播会话的模式发出，并且使用的是广播会话密钥。但是，设备通过使用了单播密钥的单播会话返回响应报文。值得注意的是所有响应报文中的序列号必须与原广播报文中的序列号相匹配。

在许多情况下，广播报文的目标地址是单个网络设备。例如，发送方想找到一个拥有某种标签的网络设备，这时只会有一个网络设备会响应该广播报文。

## 8.3.4 块数据传输

正如我们已经阐述的，WirelessHART 传输层不分解/组装大块数据报。大块数据报的分解/组装是通过应用层中的块数据传输机制来实现的。当某个设备需要发送大量数据时，它首先使用命令 799 向网络管理器请求一段时间的带宽。然后，网络管理器分配链路并回复该设备，告知该设备使用哪个路由。该设备使用该路由逐次逐块地发送块数据。最后，接收方将其组装成原块数据。WirelessHART 标准中

块数据传输规范（HCF_ SPEC-190）专门定义了如何分解和组装块数据。

### 8.3.5 传输类型代码

“网络层规范（HCF_ SPEC-085）”中的表 3 也值得阐述说明，该表的详细内容请见本书中的表 4-1。它定义了传输字节的位组合方式。常见问题是如何区分代码 1（传送响应）和代码 8（发布/通知）。它们的位设置是一样的，发送方只管发送该比特位，但这样会给接收方带来问题。解决该问题的方法是接收方的传输层不需要知道代码 1 和代码 8 间的区别，接收方的上层（应用层）能区分出这种区别。传输层在接收到这样的报文后，只需简单地转发给应用层。如果应用层期望接收一个块数据的分片，那么它就已经知道是代码 1 还是代码 8。我们应该指出的是传输字节中的序列号能给传输层提供一些线索。我们也能通过优先级来推测：数据发布（Data Publishing）的优先级高，而块数据传输（Block Data Transfer）的优先级低。

对于其他类型的报文，传输层需要知道其类型以便相应地处理。例如，当接收到一个单播响应报文的时候，传输层必须查找出与其相匹配的单播请求报文。

## 8.4 应用层

### 8.4.1 命令和报文

WirelessHART 应用层是基于命令的。应用层的载荷是一系列命令。每个命令包含一个 2B 的命令号，紧随其后的是命令本身。命令长度是由命令号决定的，因此接收方能成功地从报文中解析出每个命令。在解析了当前命令后，如果报文中仍然有数据，那么它一定是一个新命令的开始。响应报文必须包含同样的命令集，且顺序也应该是一致的。

因为网络管理器是通过命令来对网络设备进行配置，所以设备的网络层将转发命令给应用层，然后应用层理解该命令，转而再将配置指令回复给网络层。WirelessHART 网络的操作都是由应用层控制的，而应用层又受到网络管理器的管理。

命令响应数据的开始处有一个额外的状态字节。在很多情况下，响应报文复制请求报文中的内容，并将其放置于该额外状态字节之后。当一个报文中包含有多个命令请求时，因为命令响应通常比命令请求长，所以对应的命令响应报文可能无法容纳下所有这些命令的响应。在这种情况下，该报文中所有的命令请求都将不会被处理，一个全局的错误响应报文将会被返还给发送方以指明该问题。

此外，当一个报文中包含有多个命令请求时，其中的某个命令可能是无效的。这时，正确的行为是按次序地处理每个命令，并将成功的和失败的命令响应汇集成一个响应报文。设备对命令做出响应是很重要的。如果在命令被解析后，报文中还

有一些空余的字节，那么这些字节将会被响应报文忽略，并作为无效的命令而被处理。

WirelessHART 网络设备应该仅响应来自于地址 0xF981 的网关命令；WirelessHART 网络设备应该仅响应来自于地址 0xF980 的网络管理器命令；命令响应被返还给发起命令的设备，这也是非常重要的。

有时候，命令的长度是变化的，那么对应的响应命令的长度也应当与其保持一致。

### 8.4.2 无线 VS 有线命令格式

起初，HART 标准仅分配一个字节的命令号。命令格式开始于一个字节的命令号，然后是一个字节的命令数据长度，接着是一个命令数据。为了支持新命令并维持向后兼容，HART 标准后来定义了一个特殊的命令——命令 31。命令 31 意味着一个实际的命令号被定义在两个额外字节中，并被安放在命令数据长度字段之后。因此，为了解析一个有线命令报文，第一个字节需要被解读以确定命令号。如果命令号为 31，那么用户就需要从命令数据部分中找出实际的命令号。

在 WirelessHART 命令格式中，头两个字节被直接分配为命令号，随后是命令数据长度和命令数据。我们可以将有线 HART 命令转化成 WirelessHART 命令。如果命令号不是 31，那么我们可简单地设置高字节的命令号为 0，并复制命令数据。如果命令号是 31，那么我们复制数据部分中两个字节的命令并作为首先的两个字节，然后复制随后的实际命令数据。我们也能将 WirelessHART 命令转化成有线 HART 命令。如果 WirelessHART 命令的命令号小于 256，我们只需简单地移去第一个值为 0 的字节，这样该 WirelessHART 命令就变成了有线 HART 命令。如果 WirelessHART 命令的命令号大于 256，那么我们可设置命令号为 31，并在命令长度字节段后设置两个字节的命令号，接着是实际命令数据。关于状态字节，WirelessHART 中的命令响应格式也有所不同。首先，在所有响应命令之前都有一个设备状态字节和一个扩展设备状态字节。这两个字节被定义在传输层，但是可能需要被转发给应用层。有线 HART 命令没有这两个字节。真正的区别是在命令数据里。每个 WirelessHART 命令响应的头部只有一个响应代码字节；而有线 HART 命令在响应代码字节之后是一个设备状态字节。命令 0 需要被用来读取扩展设备状态。

命令解析器除了获得命令包以外，还需要被告知该命令包的版本是有线的还是无线的。命令解析器还需要知道第二个字节是否也代表着命令号。客户端以发送 HART 命令的方式来访问 WirelessHART 网关，而 WirelessHART 网关并不知道这些命令是有线 HART 命令还是 WirelessHART 命令。因此，WirelessHART 网关的开发者不得不设计某些功能，使得网关能通过查看传输介质或者其他方式来判断出客户端的命令格式。这就会给 WirelessHART 网关的开发者增加难度。

### 8.4.3　一些特别的命令

本小节解析以下一些本书其他地方没有提到的命令。

（1）命令 770　命令 770 用于打开设备发出的快速通告报文。该命名的唯一参数是快速通告的持续时间。在网络形成的初级阶段，所需要做的都是让新设备尽快地加入网络。该命令在网络形成的初级阶段是有用的，在新设备被布置并需要加入网络时也是有用的。手持设备可以发送该命令给某个网络设备，让其开始快速通告；同时，该网络设备将转发命令 770 给网络管理器，然后网络管理器又将该命令转发给所有的网络设备。

（2）命令 962　命令 962 用于向设备设置新的短地址。因为短地址被用于通信，所以对短地址的更新是一件很棘手的事情。网络管理器首先需要为网络设备及其邻居设备配置与新地址相关的所有链路，然后再改变该网络设备的短地址，最后删除与旧地址相关的所有链路。这样，该网络设备就不会成为孤点而要求重新加入网络。

（3）命令 969，974 和 976　对于某个路由 ID，它既可以是一个源路由又可以是一个图路由。命令 976 用于配置源路由，它包含有图 ID 和地址清单。命令 969 和 974 用于配置图路由。命令 969 将某个邻居设备与某个图 ID 关联起来。命令 974 将某个路由 ID 与某个图 ID 关联起来。图有多种用途。例如，从现场设备到网关的上行图路由能被用于分配给网关的路由 ID，也能被用于分配给网络管理器的其他路由 ID。通常，图应该被先创建，然后使用到该图的路由才被创建，这也导致人们坚持认为在发送命令 974 之前至少应该发送一个命令 969。

（4）命令 972　命令 972 用来终止某个网络设备。当网络设备收到该命令时，它将在某个绝对时隙数（ASN）时停止工作，然后在另一个 ASN 时恢复工作。因为设备恢复工作后首先需要重新入网，所以该网络设备回到网络的时间是不确定的。

（5）命令 64512　命令 64512 可返回射频设备制造商的信息。有时，网络设备中的无线模块不是由网络设备制造商提供的，而是由其他公司提供的。

### 8.4.4　突发数据和延时响应

设备可周期性地发布过程数据给 WirelessHART 网关，WirelessHART 网关然后将过程数据转发给上位机。本节将描述过程数据发布的建立流程。

某些 WirelessHART 命令允许延迟响应。网络设备可以利用延时响应来立即响应某个命令以表明自己正忙于执行其他事务。一旦该命令执行完毕，该网络设备将向命令的发起方发送一个最终响应报文。在这期间，设备能发送中间过程响应，命令的发起方也能通过再次发送同样的命令来查询过程。仅小部分 WirelessHART 命令允许延时响应。

WirelessHART 网络设备将按照控制系统的配置来发布数据。发布数据的频率和内容并不由网络设备本身决定，而是通过命令 101～命令 108 的一系列命令来配置。这里，我们先假设控制系统已经配置好了网络设备。

WirelessHART 网关发送命令 109（突发模式控制）给 WirelessHART 网络设备要求其开始发送突发数据。如果有足够的带宽，该网络设备会响应并立即开始发送突发数据。否则，网关将得到一个延时响应。一旦该网络设备获得网络管理器为其分配的带宽，它将发送针对命令 109 的最终响应报文给网关，然后开始发送突发数据。

这里将描述网络设备如何请求额外带宽。网络设备发送命令 799（请求时间表）给网络管理器，然后网络管理器会回复一个路由 ID 以供该网络设备使用。如果没有路由可用，该网络设备通常将会得到网络管理器发出的一个延时响应。然后，网络管理器将添加一些链路给一个新路由或一个存在的路由。最后，网络管理器把新路由的 ID 放在最终响应报文中，并将其发送给该网络设备。于是，该网络设备只能使用网络管理器指定的路由来发送突发数据。

值得注意的是我们有一个延时响应命令 799，其被封装在另外一个命令 109 中。但是，一个单独的会话应该只有一个未解决的延时响应。当网络设备等待某个延时响应时，还被允许发送其他命令。

包括命令 109 在内的命令都可用来在网络设备入网之前对网络设备进行预配置。然后，网络设备在入网后将立即发送命令 799，并与网络管理器和网关建立起正常通信。

WirelessHART 适配器会转发所有发送给其附属子设备的命令，它也可以使用延时响应。因为其附属子设备发出的响应经过有线网络传输更慢，所以适配器将先返回一个延时响应来表明命令已经被接收并正在处理中。

## 8.5 跨层相关的话题

### 8.5.1 加密算法

WirelessHART 标准采用 IEEE 802.15.4 标准定义的 CCM* 加密算法。CCM* 是 CCM 的扩展。WirelessHART 标准采用的 CCM* 加密算法实际上就是 CCM 算法。但是，WirelessHART 标准中 CCM* 算法的输入、输出参数与 IEEE 802.15.4 标准定义的输入、输出参数有所不同。对于 IEEE 802.15.4 报文解析器而言，所有 WirelessHART 报文都没有 IEEE 802.15.4 中的安全比特位，也没有被加密。其实，所有 WirelessHART 报文都是 IEEE 802.15.4 标准中的数据报文。相反，CCM* 可用于保护 IEEE 802.15.4 MAC 层的载荷，如 WirelessHART 数据。

WirelessHART 标准在两处使用了加密技术：数据链路层的认证、网络层的认证和加密。为了有利于减轻 WirelessHART 产品开发的难度和确保 WirelessHART 产品间的互操作性，我们这里将详细介绍如何使用加密算法。

### 8.5.1.1 符号的定义

WirelessHART 标准采用 IEEE 802.15.4 标准定义的 CCM* 加密算法。CCM* 是 CCM 的扩展。IEEE 802.15.4 标准中使用到的符号与加密标准（Dworkin 2004，US FIPS Publication 197）中使用到的符号略有不同。这里定义的符号遵从这两种标准。没有定义的符号是复制于 CCM 标准的。在表 8-2 中，最后两列为 WirelessHART 标准给出的合适值。

表 8-2 CCM 加密符号

| 符 号 | 定 义 | 数据链路层值 | 网络层值 |
|---|---|---|---|
| $a$ | 需认证但还没有加密的额外数据 | — | — |
| $c$ | 以字节为单位的密文 | — | — |
| $K$ | AES 加密密钥 | — | — |
| $E(K, x)$ | AES 加密函数，其中参数 $K$ 为加密密钥、参数 $x$ 为 16 个字节的明文数据串 | — | — |
| *Keylen* | 块加密密钥的位长 | 128 | 128 |
| $l(a)$ | $a$ 的字节数 | 10 ~ 121(TX)<br>13, 19, 25(ACK) | 16 ~ 49 |
| $l(m)$ | $m$ 的字节数 | 0 | 0 ~ 95 |
| $L$ | 用二进制来表示 $l(m)$ 所需要的字节数（CCM 标准称之为 $q$） | 2 | 2 |
| $m$ | 被加密的报文 | 空 | — |
| M | 消息完整性代码（MIC）的字节数 | 4 | 4 |
| MIC | 消息完整性代码。MIC 位于 $c$ 之后 | — | — |
| $n$ | 随机数（nonce）的字节数 | 13 | 13 |
| $N$ | 随机数（nonce）的字节串 | — | — |
| ‖ | 将两个位串串联起来 | — | — |
| $\oplus$ | 将两个相同长度的位串按位作异或运算 | — | — |

### 8.5.1.2 加密算法

CCM* 算法由参数 *Keylen*、$L$、$M$ 和 $n$ 定义。$a$、$K$、$m$ 和 $N$ 作为 CCM* 算法的输入参数，参数 $c$ 是 CCM* 算法的输出参数。对于加密，输入参数是 $a$、$K$、$c$ 和 $N$，而输出参数是 $m$。CCM* 是 IEEE 802.15.4 标准对 CCM 算法的一个扩展。IEEE

802.15.4-2006 中对此做了如下规定：

因此，如果 $M$ 是固定的，且 $M=0$ 是不允许的，那么参数 $N$ 将没有额外的限制，CCM*模式在这种情况下将简化成 CCM 模式。

CCM 算法要求 $L+n=15$。WirelessHART 标准定义 $n=13$，那么从该公式即可推导出 $L=2$。

CCM*算法的加密过程包含三个步骤：输入转换、认证转换和加密转换。CCM*算法的解密过程包含两个步骤：解密转换和认证检查转换。

关于 CCM*算法，WirelessHART 标准中涉及的相关章节是 TDMA 数据链路层规范（HCF_ SPEC-075）中的第 8.4 节和网络管理规范（HCF_ SPEC-085）中的第 8.1.3 节，而 IEEE 802.15.4-2006 标准中涉及的相关章节是第 7.6 节和附录 B。

#### 8.5.1.3 数据链路层的加密算法

CCM*在数据链路层被用来认证发送方发出的数据报文或接收方发出的确认报文。WirelessHART 数据链路层并不加密数据，所以由 CCM*产生的密文 $c$ 就是报文的 MIC。MIC 被放置在报文正文的末端，以形成 IEEE 802.15.4 定义的 MAC 层载荷。对于 IEEE 802.15.4 解译器而言，每个 WirelessHART 报文都是一个没有加密的数据报文。

如果发送方使用 CCM*算法来加密发送的报文，那么报文的接收方应该使用相同的 CCM*算法以及相同的输入参数。然后，接收方将自己计算出的 MIC 与报文中的 MIC 相比较。如果它们相匹配，那么该报文被认证通过，否则该报文将会被认为是无效的。

1. 输入数据

（1）$a$　不包含 MIC 和 CRC 部分的物理层载荷：

| 0x41 | 地址分类符 | 序　列　号 | 网络 ID → |
|---|---|---|---|
| → 目标地址 | 源地址 | DLPDU 分类符 | 数据链路层载荷 |

确认报文的数据链路层载荷：

| 响应代码 | 微秒级的时间调整值（最高字节在前） |
|---|---|

（2）$K$　网络内共享的网络密钥。设备入网时需要使用到如下公共密钥：7777 772E 6861 7274 636F 6D6D 2E6F 7267。

（3）$m$　其为空。

（4）$N$　如果报文中的源地址为长地址，那么 $N$ 将为

| ASN（最高字节在前） | 源地址（最高字节在前） |
|---|---|

如果报文中的源地址为短地址，那么 $N$ 将为

| ASN（最高字节在前） | 0x00 | 0x00 | 0x00 → |
|---|---|---|---|
| → 0x00 | 0x00 | 0x00 | 源地址（最高字节在前） |

2. CCM* 可被看做黑盒算法

如果使用标准的 CCM* 库，而不是使用自己开发的 CCM* 库，那么 CCM* 函数中参数 *Keylen*、$L$、$M$ 和 $n$ 就必须使用上述定义的值。然后，CCM* 函数产生的密文 $c$ 就是 MIC，该 MIC 将会被放置在数据链路层帧中。

3. WirelessHART 专用的 CCM* 函数

以下是按照 WirelessHART 标准简化后的 CCM* 加密算法：

（1）输入转换

1）将 $l(a)$ 编码为 2 个字节的八位字节串 $L(a)$。

2）将 $L(a)$ 接在八位字节串 $a$ 后面。

3）在上述字节串后补最少的零直到总长度能被 16 整除，形成填补后的 AuthData。

（2）认证转换

1）构造含 16 个八位字节的 $B_0 = 0x49 \parallel N \parallel 0x00 \parallel 0x00$。

2）将 AuthData 报文划成 $B_1 \parallel B_2 \parallel \cdots \parallel B_t$，每个 $B_i$ 块是 1 个含 16 个八位字节的字节串。

3）CBC-MAC 值 $X_{t+1}$ 是被定义成 $X_0 := 0^{128}$；$X_{i+1} := E(K, X_i \oplus B_i)$，其中 $i = 0, \cdots, t$。字节串 $0^{128}$ 是 1 个含 16 个全零的八位字节的字节串。

4）认证标签 $T$ 是由此产生的 $X_{t+1}$ 最左边的 1 个含 4 个八位字节的字节串。

（3）加密转换

1）构造含 16 个八位字节的 $A_0 = 0x01 \parallel N \parallel 0x00 \parallel 0x00$。

2）定义含 16 个八位字节的加密块 $S_0$ 为 $S_0 := E(K, A_0)$。

3）如果以上任何一步操作失败则输出"invalid（无效）"，否则把 $S_0$ 最左边的 1 个含 4 个八位字节的字节串与认证标签 $T$ 异或而产生加密后的认证标签。该标签就是返回的 MIC。

#### 8.5.1.4　网络层加密算法

每个报文的网络层载荷都需使用 CCM* 加密。源设备加密报文的网络层载荷，而目标设备解密报文的网络层载荷。数据传输路径上的路由设备仅简单地转发已加密的载荷。不像数据链路层的载荷，网络层载荷是被加密的，所以报文的目标设备需调用 CCM* 的解密部分以还原出报文。

1. 输入数据

（1）$a$　它是网络协议数据单元（NPDU）的头部。其起始于 NPDU 中的控制

字节字段，终止于 NPDU 中的 MIC 字段。当加密 NPDU 时，TTL、计数器和 MIC 字段的值都需设置为 0。而在报文被传送之前，这些字段的值将会被恢复成真实值。

| 控 制 | 0x00 | ASN 片段 | 图 ID | 目 标 地 址→ |
|---|---|---|---|---|
| →源地址 | [扩展路由信息] | 安全控制 | 0x00 or 0x00，0x00，0x00，0x00 | 0x00，0x00，0x00，0x00 |

（2）*K*　源设备与目标设备间共享的会话密钥。设备在加入网络时 *K* 采用加入密钥。

（3）*m*　NPDU 中的载荷。

（4）*N*　如果报文中的源地址为长地址，那么 *N* 将为：

| 0x01（加入网络时），<br>0x00（其他情况时） | 随机数（nonce）<br>计数器（最高字节在前） | 长地址（最高字节在前） |
|---|---|---|

如果报文中的源地址为短地址，那么 *N* 将为：

| 0x01（加入网络时），<br>0x00（其他情况时） | 随机数（nonce）计数器（最高字节在前） | 0x00，0x00，0x00，0x00，0x00，0x00 | 短地址（最高字节在前） |
|---|---|---|---|

注意：随机数（Nonce）计数器是发送方的 4 个字节的计数器。根据情况不同，数据报中随机数（Nonce）字段的长度有可能为 1 个字节或 4 个字节。如果是 1 个字节，那么接收方应该提供其他 3 个高位字节，这意味着接收方必须清楚数据报中这个字节何时发生溢出。

按照 WirelessHART 标准的要求，用于加密入网响应报文的随机数由入网请求中的随机数计数器和新设备的长地址构建。这与用于其他报文的随机数不同。其目的是为了增加安全性。

2. 将 CCM* 看作一个黑盒算法

如果你调用一个标准的 CCM* 库而不是自行开发 CCM* 库，那么你需要选择使用上述 *Keylen* 、*L* 、*M* 和 *n* 参数值的 CCM* 函数。这样，该 CCM* 函数的返回值 *c* 就是加密后的载荷和右接的 MIC 。加密后的载荷应放在 NPDU 载荷的位置；4 个字节的 MIC 应放在 NPDU 载荷前的位置。接收方将加密后的 NPDU 载荷右接 4 个字节的 MIC 来构成 *c* 。如果解密成功，返回值 *m* 就是解密后的载荷。

3. 根据 WirelessHART 标准修改后的加密算法

以下是按照 WirelessHART 标准简化后的 CCM* 加密算法：

（1）输入转换

1）将 $l(a)$ 编码为 2 个八位字节的字节串 $L(a)$。

2）将 $L(a)$ 接在八位字节串 $a$ 后面。

3）在上述字节串后补最少的零直到总长度能被 16 整除，形成填补后的 AuthData。

4）在 $m$ 后补最少的零直到总长度能被 16 整除，形成填补后的 PlaintextData。

5）由 AddAuthData 和 PlaintextData 构造成数据报 AuthData：AuthData = AddAuthData ‖ PlaintextData。

（2）认证转换

1）构造含 16 个八位字节的 $B_0$ = 0x49 ‖ $N$ ‖ 0x00 ‖ 0x00。

2）将 AuthData 报文划成 $B_1 \| B_2 \| \cdots \| B_t$，每个 $B_i$ 块是 1 个含 16 个八位字节的字节串。

3）CBC-MAC 值 $X_{t+1}$ 是被定义成 $X_0 := 0^{128}$；$X_{i+1} := E(K, X_i \oplus B_i)$，其中 $i = 0, \cdots, t$。字节串 $0^{128}$ 是 1 个含 16 个全零的八位字节的字节串。

4）认证标签 $T$ 是由此产生的 $X_{t+1}$ 最左边的 1 个含 4 个八位字节的字节串。

（3）加密转换

1）构造 16 个八位字节的 $A_i$ = 0x01 ‖ $N$ ‖ 0x00 ‖ 计数值 $i$，其中 $i = 0, 1, 2, \cdots$。

2）将 PlaintextData 报文划成 $M_1 \| \cdots \| M_t$，其中每个 $M_i$ 块是 1 个含 16 个八位字节的字节串。

3）加密块 $C_1, \cdots, C_t$ 被定义成 $C_i := E(K, A_i) \oplus M_i$，其中 $i = 1, 2, \cdots, t$。

4）Ciphertext 串等于字节串 $C_1 \| \cdots \| C_t$ 去掉最左边的 $l(m)$ 个字节。

5）构造含 16 个八位字节的加密块 $S_0$ 为 $S_0 := E(K, A_0)$。

6）加密后的认证标签 $U$ 等于 $S_0$ 最左边的含 4 个八位字节的字节串与认证标签 $T$ 的异或。

7）如果以上任何一步操作失败则输出"invalid（无效）"；否则，输出的 $c$ 是加密后的报文，输出的加密后的认证标签是 MIC 。

4. 根据 WirelessHART 标准修改后的解密算法

以下是按照 WirelessHART 标准简化后的 CCM* 解密算法：

（1）解密转换

1）在加密载荷后补最少的零直到总长度能被 16 整除，形成填补后的报文 CiphertextData。

2）使用前面关于加密一节中的加密转换，输入值采用 CipherTextData 和标签 $U$，即收到报文中的 MIC 。

3）将该转换产生的字节串看成 $m \| T$，其中最右边的 $T$ 是 1 个含 4 个八位字节的字节串。$T$ 是所谓的认证标签。

（2）认证检查转换

1）使用前面关于加密一节中的输入转换构造 AuthData 报文，输入值采用 $a$ 和

解密转换中产生的字节串 $m$ 。

2）使用前面关于加密一节中的认证转换，输入值采用 AuthData。

3）将该转换输出的标签 MACTag 与上述解密转换建立的标签 $T$ 相比较。如果 MACTag = $T$，输出“valid（有效）”；否则，输出“invalid（无效）”并停止解密。

（3）输出

1）如果以上任何一步操作失败则输出“invalid（无效）”；否则，接受解密后的字节串 $m$ 。

#### 8.5.1.5 加密密钥的生存时间

CCM 算法要求在某一情况下（比如在加密密钥的有效生存时间内）一个 $N$ 值只能使用一次。这就限制了加密密钥的有效生存时间。WirelessHART 标准规定了加密密钥的更换。因此，加密密钥在到达该有效生存时间前就会被更新。

在数据链路层，密钥在 WirelessHART 网络内共享。参数 $N$ 包含了 ASN 和源地址。这意味着只要 ASN 没有溢出，该密钥就能一直被使用。ASN 是用来统计时长 10 ms 的时隙数的 5 个字节序列号，它溢出所需要的时间是三个多世纪。因此，这方面的问题可以不需要考虑。

在网络层，密钥被源设备与目标设备之间的会话共享。参数 $N$ 包含了一个 4 个字节的随机数计数器和源地址。这意味着密钥在随机数计数器溢出之后必须更换。随机数计数器的溢出意味着 40 亿个报文。如果设备每个时隙都发送一个报文，那么它发送完 40 亿个报文将需要一年的时间。像数据链路层一样，这方面的问题也不需要考虑。

#### 8.5.1.6 渐进执行

在 WirelessHART 标准中，一次双向通信要求在 10 ms 的时隙内完成。在数据链路层，对于最长的报文，接收方也必须认证该报文，并在 1ms 内准备好 CCM* 加密后的确认报文。对于接收方，及时地执行此任务是非常有挑战性的。此外，接收方的处理能力可能比较低，它可能由电池供电。WirelessHART 设备被期望能够是低功耗和长续航时间的。

这种加密是 WirelessHART 标准特有的。IEEE 802. 15. 4 标准中 MAC 层的确认机制并没有涉及加密。接收方不需要处理收到的报文再回复。格式为“Frame Control + Sequence Number + FCS”的确认报文没有被加密。

加密方式是 CCM（Dworkin 2004）。该标准有如下描述：“CCM 是为了在包环境中使用而设计的，例如，在使用 CCM 之前，所有数据在存储器中是可用的。CCM 不是为支持部分数据处理或流处理而设计的”。这么描述的主要原因是参数 $a$ 和 $m$ 的长度必须首先被加密。然而，由于 WirelessHART 标准规定的方式，在整个报文存在很久之前，我们就知道参数 $a$ 和 $m$ 的长度。我们能按照 16 字节的块的方式来处理正到达的报文。我们不需要等到直到整个报文被接收到后才开始执行 CCM 算法。一旦

MAC 层报文头部被接收到，我们就可以开始创建出 Authentication transformation（认证变换）中的第一个八位字节 $B_1$。MAC 层报文包含 $B_1$ 所需的报文长度。

然后，随着报文的流入，我们能创建长 16 个字节的 $B_i$ 序列。同时，创建出的 $B_i$ 能被提供给 CCM 加密算法。CCM 认证包含一系列基于 16 字节块的 AES 加密程序。如果我们假设处理器运行 CCM* 程序的速度能快过数据流的到达速度，数据流的到达速率为 32μs/B，那么在使用渐进运算的情况下，在报文结束与确认报文开始之间只要对最后的 $B$ 块和 $A_0$ 块做 AES 计算。

下一步，我们认为对 $A_0$ 块的计算也可以移到响应区间之外。我们事先执行一些对收到报文和确认报文的处理。

对收到报文，接收方可以在报文进来前就创建 $A_0$。因此我们可以提前对 $A_0$ 进行计算。

对确认报文我们也可以提前对 $A_0$ 进行计算。$B_0$ 也可以被提前计算因为它的长度是固定的。如果报文中的源地址和目标地址都是短地址，则确认报文只有一个数据块 $B_1$。否则只有两个数据块 $B_1$ 和 $B_2$。如果有两个数据块，则 $B_1$ 的内容可以提前确定。而对提前确定的块，我们可以提前对它进行 AES 计算。总之，在处理完收到报文后只有一个 $B$ 块需要加密。

更多的观察结果：

（1）发送方也可以用此方法提前计算发送报文。发送方可以在实际发送时隙到来前就把报文加密好。发送方可以在空时隙进行密度大的加密计算。在计算中必须使用实际发送时隙的 ASN 值而不是加密计算时的 ASN 值。

（2）$A_0$ 仅在 WirelessHART 数据链路层被使用到。在其他情况下，我们可以在实际加密运算前计算 $A_i$ 块执行 AES。比如，这可用于 WirelessHART 网络层和其他使用 AES 的地方。

（3）如果某个网络设备不是时钟源，我们可以把它的 timeAdjust 设成 0。那么确认报文中唯一未知的值就是响应代码（Response Code），而响应代码只能是四个值之一。这儿有两种选择。我们可以事先计算出所有四种确认报文，然后根据收到的报文决定发送哪个。我们也可以事先产生成功状态的确认报文。如果需要确认失败的确认报文，那么我们可以选择不发确认报文。换句话说，用不回答表示拒绝。

（4）当渐进加密报文时，我们也可以同时计算 CRC 以进一步减少在接收方短暂回应期间的计算量。

在我们利用 FreeScale 芯片成功实现 Wi-HTest™ 测试工具中，我们就是采用的渐进加密方式。Wi-HTest 工具是 HCF 测试工具箱的一个重要组成部分。这个 Wi-HTest 工具用于测试和评估某个产品是否符合 WirelessHART 标准。

#### 8.5.1.7 硬件加速

市场中符合 IEEE 802.15.4 标准的大部分芯片都为加密提供了硬件加速功能。

只要芯片中的硬件加速允许常规的 CCM 或 AES 算法而不是直接加密一个 IEEE 802.15.4 报文，那么 WirelessHART 产品就能使用该芯片。如果只有 AES 是硬件实现的，那么 CCM*实现的其余部分仍然需要通过软件代码来实现。

因为 WirelessHART 在两层都使用了 CCM*，所以有必要保证整个加密计算是一个整体单元。一个 CCM*很可能将多次使用硬件加速器来完成一个报文的加密。在网络层执行 CCM*的过程中，如果数据链路层开始使用该硬件加速功能，那么网络层需要重新开始执行 CCM*。

### 8.5.2 报文生存时间

报文的实际生存时间由以下几个因素决定：

（1）TTL　TTL（生存时间）实际上是生存跳数。它定义了报文能够被转发的跳数，该值被存放在网络层的头部中。每当报文被传送 1 次，TTL 值就减 1。如果 TTL 值达到 0 时，那么该报文就会被丢弃掉。

（2）maxPacketAge　maxPacketAge 是一个被网络管理器预先配置的网络层属性。WirelessHART 网络设备将 maxPacketAge 与报文的年龄相比较，如果报文的年龄大于 maxPacketAge，那么该报文就被丢弃。maxPacketAge 与报文年龄的基本单位都是时隙数。

（3）retryCount 和 responseTimer　retryCount 和 responseTimer 也是被网络管理器预先配置的网络层属性。在 responseTimer 之后，报文被认为死亡。然后，一个再生的报文被发出直到达到 retryCount 值。TTL 和 maxPacketAge 共同确定了一个报文的生存时间。responseTimer 应该大于 maxPacketAge。对于一个来自于应用层的请求，其最长生存时间为 retryCount 乘以 responseTimer。

### 8.5.3 重传

WirelessHART 标准在数据链路层和网络层都提供了重传机制以处理传送失败。数据链路层重传报文直到该报文被转发给下一个邻居设备。网络层重传报文直到接收到对方设备的响应报文。这两种重传机制都有时间限制。作为超时的结果，失败将会被报告。

在数据链路层，从网络层来的报文将与一个超时时间值相关联。一有可用的合适链路，数据链路层就将试着发送该报文。如果由于 CCA 问题、没有接收到确认或确认报文中指示的拒绝而导致传送失败，那么数据链路层将在下一个可用链路重发该报文直到成功或超时时间值溢出（即超时）。

从网络层来的超时时间值是基于报文中的 ASN snippet 和 maxPacketAge 计算出的。报文创建时的 ASN 值加上 maxPacketAge 即为报文的生存时间。ASN snippet 和 maxPacketAge 长度都是两个字节。如果 maxPacketAge 很大，则要避免在从 snippet

构造 ASN 时发生 snippet 溢出的错误。数据链路层简单地重传直到报文不再被允许存在。

如果某个设备的网络层只是简单地转发报文，那么该设备的网络层不会主动重传转发的报文。数据链路层返回一个超时指示时，即意味着对应的报文已经死亡了。如果某个设备的网络层是报文源，并且发出的报文要求响应，那么该设备的网络层会要求重传没有收到响应报文的报文；如果在超时之前仍没有接收到响应报文，那么该设备的网络层将重传一次；即使该设备的网络层早已意识到报文的传送失败，但是它被建议应该等待直到超时。如果重传计数器达到阈值，那么该报文将会被认为是无法送达的，将会返回给上层一个错误。

对于不需要确认的广播报文，一旦它们被无线发送出去了，那么它们就被认为被成功地传送了。

## 8.5.4 MSB 和 LSB，大端和小端

如果仔细研究一个完整的 WirelessHART 报文，那么将会注意到在数据链路层和网络层之间两个字节的设备地址遵照不同的顺序。例如，如果设备地址是 0x0123，那么在数据链路层头部中 0x01 字节会位于 0x23 之后，但是在网络层头部中 0x23 字节位于 0x01 之后。这是因为 IEEE 802.15.4 标准遵循“小端（Small endian）”格式，而 HART 标准遵循“大端（Big endian）”格式。WirelessHART 标准为了顺应 IEEE 802.15.4 标准，所以当创建数据链路层头部的时候，WirelessHART 标准不得不使用“Small endian”格式。但是，数据链路层载荷中的任何数据还是遵循“Big endian”格式。

“endianness”是什么？根据 IEEE 标准术语的权威字典，“endianness”定义为“Big endian 是多字节数字值的一种表示方式，即存放在内存地址中最低位的数值是来自数据的最左边部分（也就是数据的最高为部分）。Small endian 也是多字节数字值的一种表示方式，即存放在内存地址中最低位的数值是来自数据的最右边部分（也就是数据的最低位部分）”。

在 WirelessHART 报文中，前面的字节对应着更低的存储地址。

用以描述“endianness”的另一组更常见术语被称为“第一位是最高有效字节（Most Significant Byte（MSB）First）”和“第一位是最低有效字节（Least Significant Byte（LSB）First）”。“Most Significant Byte（MSB）First”也称为“Big endian”，而“Least Significant Byte（LSB）First”对应着“Small endian”。

Wikipedia™ 网站 http://en.wikipedia.org/wiki/Endianness 上能找到更详细的关于“endianness”词条的解释。不像 IEEE 标准组织，HART 标准组织是一个工业联盟。HART 标准组织的一个关键职能是培训人们以推广标准。尽管有围绕 Wikipedia 权威性的争论，但是 Wikipedia 网络上“endianness”词条被 HART 标准组织认

为是非常有用的，并被包含在 WirelessHART 文档中。

由于两者都在 WirelessHART 标准中存在，我们在形成或解读 WirelessHART 报文的时候应该非常小心。例如，ASN 必须是 MSB 格式的。应用层命令中的任何数据都必须遵循 MSB 格式。

经验法则：在 WirelessHART 标准中，除了遵循 IEEE 802.15.4 标准的部分应该是 LSB 格式的，其余部分都应该表示成 MSB 格式。

这无疑导致了编程中的潜在陷阱。当形成或还原一个多字节整数时，程序员必须要知道是使用 MSB 还是使用 LSB。

令事情更糟糕是多字节整数本身可能被按照 MSB 或 LSB 格式存储在存储器中。然而，按照 MSB 还是按照 LSB 格式存储，则依赖于使用的处理器。例如，Intel 的 PC 处理器是“Small endian”格式的，而大部分嵌入式处理器是“Big endian”格式的。对于 WirelessHART 报文中的整数，基于 Windows 操作系统的应用程序与 WirelessHART 网络设备中的应用程序在处理方式上完全相反。

字节里的位顺序有时候也是难以理解的。事实上，IEEE 802.15.4 标准定义 LSB 为最低有效位，并用其描述如何发送数据位，即最低有效位最先被发送。譬如，所有 WirelessHART 报文都是 IEEE 802.15.4 数据报文类型。如果源地址和目标地址都是短地址，那么 HART 标准中图 35 中的 16 位帧控制字段被表示为 1000001000010001，也按照这个顺序发送。然而，当看作两个字节时，它们分别是 0x41 和 0x88。实数将按照 HART 标准严格地表示为字节的序列，这里应该没有混淆。

### 8.5.5 短地址和长地址

为了符合 IEEE 802.15.4 标准，WirelessHART 标准支持长地址和短地址。当设备入网的时候，两个字节的短地址由网络管理器动态分配。像任何网络设备的 MAC 地址一样，8 个字节的长地址对于每个 WirelessHART 设备而言都是唯一的。WirelessHART 设备的长地址是固定的，且与世界上所有其他 HART 设备的长地址不同。长地址由 5 个字节的 HART 唯一 ID 和分配给 HART 基金会的 3 个字节的“组织唯一标示符”（Organizationally Unique Identifier，OUI™）组合而成。长地址仅在设备入网的时候被使用到。一旦设备收到了分配给自己的短地址，那么它就应该停止使用长地址。这样做的原因是长地址从来不会被用于配置网络设备。设备只与拥有短地址的邻居设备建立链路。长地址与短地址之间的地址映射仅保存在网络管理器中。网络管理器甚至不可能维护该地址映射。如果某个设备接收到一个报文，而该报文中的源地址为长地址，那么该设备无法将该地址与任何已知的邻居设备关联起来。

网络管理器发送入网响应报文给入网设备，该响应报文会包含有网络密钥和短

地址。如果报文中的源地址或目标地址是长地址，那么用来认证该报文的密钥肯定是公共密钥。因此，我们可以据此来确定该报文中使用的是公共密钥还是网络密钥。

## 8.5.6　随机数计数器和序列号

WirelessHART 标准定义了三个号码来跟踪报文通信：数据链路层的 IEEE 802.15.4 数据序列号、网络层的随机数（nonce）计数器和传输层的序列号。每个号码的用途都不尽相同。

### 8.5.6.1　IEEE 802.15.4 数据序列号

IEEE 802.15.4 MAC 层帧头的第三个字节是数据序列号（Data Sequence Number DSN）。每个设备随机产生该数据序列号，并存储于本地。每当报文形成的时候，数据序列号被复制到报文中并加 1。自动应答报文必须从原报文中复制出该数据序列号。数据序列号在 256 个时隙（即 2.56 s）后会溢出。

WirelessHART 标准在这方面与 IEEE 802.15.4 标准稍微有所不同。ASN 普遍存在于 WirelessHART 网络。ASN 的最低有效字节（LSB）被用作 WirelessHART 报文的序列号。对于在某个时隙内发送的报文，不管该报文是由哪个设备发出还是在哪个信道传递，报文的序列号都是同一个确定的值，即 ASN 最低有效字节。这提供了一些避免干扰的保护措施。如果报文的序列号与其发送时的时隙号不匹配，那么一定有错。WirelessHART 标准没有采用 IEEE 802.15.4 标准中的自动应答机制。然而，WirelessHART 标准要求确认报文的序列号与其发送时的时隙号相匹配。在 WirelessHART 标准中，序列号并不是随着发送报文数量的增加而持续累加的，它在 256 个时隙（即 2.56 s）后会溢出。

### 8.5.6.2　随机数计数器

网络层定义了 4 个字节的随机数计数器。每个设备的每次会话都有一个随机数计数器。随机数计数器被用于跟踪报文流。会话中的每个新报文都会与当前的随机数计数器关联起来。在每个报文形成之后，随机数计数器的值会被加 1。针对报文的无序到达或丢失，WirelessHART 标准采用滑动窗口算法来改善通信和消除重复数据报。在 WirelessHART 标准中，接收方可以记录下发送方的随机数计数器值，并以此随机数计数器值为基准，维护着一个 32bit 的前向滑动窗口。接收方每次接收到一个报文后，都将该报文中的随机数计数器值与记录下的随机数计数器值进行比较。如果报文的随机数计数器值大于记录下的随机数计数器值，那么接收方就将记录下的随机数计数器值更新为该报文的随机数计数器值。如果报文中的随机数计数器值加上 32 后仍小于记录下的随机数计数器值，那么接收方就直接丢弃该报文。这样，接收方就可以识别出哪个报文提早到达、哪个报文还没有达到。

随机数计数器对于安全来说也是非常重要的。它被用于构建随机数。为了加密

和认证，随机数被用于 CCM*算法。4 个字节的随机数计数器确保了随机数仅会在 $256^4$ 个报文后会溢出。考虑到时隙时间长度为 10 ms，那么随机数计数器溢出的最早时间是 $256^4/100$ s（即 1.3 年）。

为了节省报文的开销，在正常会话通信中，报文中仅包含了随机数计数器的低有效字节。这意味着接收方必须准确地保存着发送方随机数计数器中的 3 个高位字节。因此，接收方需要完成两个任务：一个任务是获得对方随机数计数器中 3 个高位字节的初始值；另一个任务是每当最新报文中的随机数低有效字节溢出时更新该 3 个高位字节。

网络管理器通过向网络设备写入命令 963（写会话命令），就可以与该设备建立起了一个会话。正常情况下，命令 963 包含了会话对方的随机数计数器值。这样，设备就知道了会话对方随机数计数器中 3 个高位字节的初始值。当接收到命令 963 的时候，设备也将自己的随机数计数器设置为 0。这样，如果设备的会话对方是网络管理器或网关，那么网络管理器或网关也能知道设备随机数计数器的 3 个高位字节。目前，在 WirelessHART 标准中，所有会话的一端都是网络管理器或网关。如果未来版本的 WirelessHART 标准支持设备与设备间的会话，那么网络管理器就需要向会话两端的每个设备写入命令 963。这时，因为命令 963 仅用于设置会话双方的随机数计数器，所以发送给两个设备的命令都必须将随机数计数器的值设置为 0。

在设备加入网络的过程中，例如对于入网会话，入网请求报文和入网响应报文都包含了一个完整的 4 字节随机数计数器值。实际上，网络管理器在入网响应报文中必须使用相同的随机数值以预防攻击。设备将入网响应报文中接收到的随机数计数器值与请求报文中使用的值相比较。如果它们不匹配，那么设备就认为该响应报文是无效的。

接下来，当随机数的低有效字节溢出时，我们将讨论设备如何更新其会话对方的随机数的 3 个高位字节。假设接收方收到了发送方发出的两个报文：报文 A 和报文 B，其中报文 A 是接收方刚收到的报文，报文 B 是之前收到的报文。在报文 A 中，随机数低有效字节的值为 $x$；在报文 B 中，随机数低有效字节的值为 $y$。当 $x$ 大于 $y$ 时，接收方会认为报文 A 是在报文 B 之后发出的；当 $x$ 小于 $y$ 时，接收方会认为报文 A 是在报文 B 之前发出的。在本假设中，因为报文 A 是最新的报文，所以 $x$ 应该大于 $y$，但是由于随机数计数器溢出的原因，$x$ 既可能大于又可能小于 $y$。例如，我们假设 $x$ 大于 $y$，报文 A 可能是报文 B 之后第 $x-y$ 个报文，也可能是报文 B 之前第 $256-(x-y)$ 个报文。报文 A 和报文 B 的随机数值通常不应该相差很大。如果报文 A 和报文 B 的随机数值相差很大，那么报文 A 和报文 B 之间的报文可能都丢失了，这样发送方由于长期没有收到响应报文而会终止会话，从而也就不可能再发出报文 B。基于这一常理，我们应该选取 $x-y$ 和 $256-(x-y)$ 中的较小值。例

如，当报文 A 中的随机数低有效字节值 $x$ 等于或接近于 255，而报文 B 中的随机数低有效字节值 $y$ 等于或接近于 0，那么接收方应该很容易地推断出报文 B 是在报文 A 之后发出的，而且发送方的随机数的低有效字节发生了溢出。

如果设备（例如运行于工作站上的网关或网络管理器）拥有足够的计算资源，那么它可以尝试做两次 CCM* 运算。对于随机数的 3 个高位字节，其中一次 CCM* 运算假设这 3 个高位字节的值没有变化；而另一次 CCM* 运算假设这 3 个高位字节的值为当前值加 1。对于这两次的运算结果，哪次结果通过了认证就可以认为其对应的假设成立，因为两次结果同时都能通过认证的情况是不可能发生的。

#### 8.5.6.3 WirelessHART 序列号

WirelessHART 传输层控制字节的低 5 位是传输层序列号。依照 WirelessHART 标准："对于无确认通信，传输层序列号应该被设置成包计数器（PacketCounter）的 5 位低有效位。当传输表被建立的时候，包计数器的值被初始化为 0。然后，每当一个无确认包被通过该传输管道传输，包计数器的值就被累加 1"。

WirelessHART 标准对确认报文中的传输层序列号要求非常严格。每个通信对，即发送方和接收方，都维护着一个属于它们自己的序列号，并在每次报文传送后加 1。接收方必须从接收到的报文中复制出序列号，然后将该序列号放置到自己的确认报文中。按照 WirelessHART 标准的要求，接收方仅接受这样的报文，即报文中的序列号等于前次报文中的序列号加 1。设备在任何时候都只能最多有一个未确认的报文，这是 WirelessHART 标准强制要求的。一旦某个报文得到了确认，那么设备就可以开始发送下一个报文了。但是，延迟响应是一个例外。同一个报文可以对应有多个延迟响应报文，最后一个延迟响应报文能在许多其他报文完成后才被传送。即使对于延迟响应，发送方也必须在接收到第一个延迟响应报文后，才能发送下一个报文。WirelessHART 序列号在 $2^5=32$ 个报文后就会发生溢出。

如果发送方和接收方之间失去了序列号同步，那么它们之间的会话将成为无用的了，一个新的会话必须被创建以重新建立起它们之间的通信。例如，如果某个确认报文在网络中丢失了，那么会话将会被中断，因为这时发送方继续使用之前的序列号，而接收方期望的是下一个序列号。

重新建立一个会话的代价是很高的，所以设备可以尝试一些办法来避免会话的中断。例如，如果没有收到接收方返回的响应报文，那么发送方可以尝试使用不同的序列号，即发送方使用不同的序列号重新发送相同的报文，直到接收方响应或超时。当前序列号的下一个序列号是应该被发送方选来尝试处理上述情况的。发送方也可以尝试使用其他序列号，例如当前序列号之前和之后的序列号。对于接收方接收到的报文，即使该报文中的序列号不是接收方期望的下一个序列号，接收方仍将处理该报文。按照 WirelessHART 标准规定，接收方应该拒绝所有非其所期望的报文。但是，在具体实现 WirelessHART 协议时，如果接收报文中的序列号小于或接

近于期望的序列号，那么接收方可以接受该报文并将该序列号作为新的正确序列号。

由于发送方在传输层有重传机制，那么接收方可能会接收到重复的报文。当接收方接收到重复报文时，即使报文及重复报文中的序列号并不是接收方所期望的，只要报文及其重复报文的序列号相一致，接收方就将认可该报文及其重复报文。这样也就能维护着会话的持续。

### 8.5.7 时间戳和 ASN 时间

WirelessHART 网络是完全同步的。一个时隙正好是 10ms。当 WirelessHART 网络被创建的时候，ASN 为 0，即 ASN0。所有设备都准确地知道网络被创建时的时间，即 ASN0 对应的实际物理时间。如果一个设备知道 ASN0 对应的实际物理时间，那么该设备就能准确地推算出当前的实际物理时间。这样，在打时间戳或对网络事件排序时将不成问题。命令 793（Write UTC Time Mapping）能告诉设备网络创建时间 ASN0 对应的实际物理时间。

### 8.5.8 主设备和从设备

在 WirelessHART 网络中，主设备是发出请求命令的设备，而从设备是响应请求命令的设备。这也遵循了早期有线 HART 标准的定义。通常，网络管理器和网关是主设备，现场设备是从设备。网络管理器或网关发出的报文包含了命令数据，而现场设备发出的报文包含了命令响应数据。新设备发出的入网请求报文包含了命令响应数据，也被认为是一个响应。入网请求报文的响应报文实际上包含有发给新设备的三个命令，新设备收到这三个命令后应该发出一个命令响应报文。

然而，在某些特殊的情况，现场设备是主设备而网络管理器是从设备。命令 799（Request Timetable）就是其中的一个例子。设备发送该命令给网络管理器以请求带宽，网络管理器会回复一个路由 ID 给该设备以便其用于数据通信。另外一个实例是命令 770（Request Active Advertising），该命令主要用于手持设备。

### 8.5.9 广播和单播

网络层定义了广播报文和单播报文。数据链路层定义了广播链路和单播链路。这样，报文传送方式就存在着多种不同的组合：网络层单播报文被发送在一个普通的单播链路上、网络层广播报文被发送在一个广播链路上、网络层单播报文被发送在一个广播链路上、网络层广播报文被发送在一个普通的单播链路上。这些报文传送方式在 WirelessHART 标准中都是合法的。请参见“网络规范”中的表 19。

广播报文的网络层头部中的目标地址都是统一的，即 0xFFFF。单播会话中的目标地址既用于发送报文也用于接收报文。广播会话中的目标地址既可以是网关的

地址，也可以是网络管理器的地址。对于广播报文而言，其源地址是网络管理器或网关的地址，其目标地址是 0xFFFF。当设备收到并转发一个广播报文时，转发出的广播报文的源地址和目标地址与接收到的广播报文的源地址和目标地址应完全一致。

## 8.6 其他话题

### 8.6.1 存储空间

WirelessHART 标准是一个工业级的标准。其涵盖的许多特色有时候提供了一些自相矛盾的要求，例如节能与实时响应。相对于其他低功耗、低数据率的无线网状网络，WirelessHART 协议栈需要更大的存储空间。因此，市场上的一些 IEEE 802.15.4 处理器可能无法满足 WirelessHART 协议栈的需求。例如，我们的实际开发经验表明，飞思卡尔的 MC1321™处理器不适合于 WirelessHART 协议栈的实现。其中一个主要原因是该处理器只有 8KB 的 RAM，这对于 WiressHART 协议栈而言太小了。为了开发 WirelessHART 测试系统，我们曾经尝试在 JM128™ Codefire™处理器上实现 Wi-HTest 测试工具。即使 Wi-HTest 没有实现完整的 WirelessHART 协议栈，我们仍不得不努力控制数据量的大小使其不超过 20KB 的 RAM。

接下来，我们将使用我们自主开发的 Wi-HTest 作为参考来估算 WirelessHART 数据结构所需要的内存空间。

1. 数据链路层

在数据链路层规范㊀中的表 4 定义了最小表和缓冲区需求。这里，我们将其复制成表 8-3。

表 8-3　最小表和缓冲区的需求

| 描　述 | Wi-HTest 工具中的大小/B | 最低要求/B |
|---|---|---|
| 邻居 | 21 | 32 |
| 超帧 | 12 | 16 |
| 链路 | 21 | 64 |
| 图 | 8 | 32 |
| 图-邻居节点对 | 4 | 128 |
| 包缓冲区 | 196 | 16 |

㊀ 相关规范的名称和编号见参考文献，读者可自行查找。——译者注

将以上全部加在一起，存储空间大小总计为6112B。

2. 网络层

在网络层规范中[⊖]的表14定义了最小表的空间需求。这里，我们将其复制成表8-4。

表8-4 最小表的空间需求

| 描　述 | Wi-HTest 工具中的大小/B | 最低要求/B |
|---|---|---|
| 会话 | 53 | 8 |
| 对应的设备 | 2 | 1（每个会话） |
| 传输表 | 13 | 2（每个会话） |
| 路由 | 27 | 8 |
| 源路由 | 17 | 2 |
| 时间表 | 13 | 16 |

将以上全部加在一起，存储空间大小总计为1106B。

因此，存储数据链路层和网络层所需的数据结构就至少需要7KB的RAM。

## 8.6.2 密钥更换

出于安全原因，密钥必须要周期性地更换。这里，我们讨论两种密钥的更换：数据链路层的网络密钥和网络层的会话密钥。这两种密钥是分别通过命令961和命令963来设置的。

通常，每个设备有四种会话密钥：到网络管理器的单播会话密钥和广播会话密钥，到网关的单播会话密钥和广播会话密钥。这里，我们仅讨论在网络正常运行期间新密钥如何生效。入网密钥仅用于入网期间，故在此不讨论。

### 8.6.2.1 数据链路层的网络密钥

命令961被网络管理器用来通知设备启用新的密钥。命令961中包含有一个ASN值，该值意味着所有网络设备从该ASN时刻开始都将开始使用新密钥。因为网络密钥被网络中所有的设备共享，所以网络管理器必须要十分小心地选取一个合适的ASN值，以确保命令961能在该ASN之前被所有网络设备执行完毕。

1）如果命令961中的ASN是将来的，那么将会执行正常操作。

2）如果命令961中的ASN为0或ASN值丢失了，那么设备将立刻转换到使用新密钥。这主要针对新设备加入网络的情况。在入网过程中，新设备只要接收到入网响应，就立即转换到使用新密钥。

⊖ 相关规范的名称和编号见参考文献，读者可自行查找。——译者注

3）如果命令 961 中的 ASN 在当前 ASN 之前，那么设备将回复错误代码 0x42，丢弃该命令，并继续使用当前的密钥。

#### 8.6.2.2　网络层的会话密钥

命令 963 实际上用于写一个新的会话。命令 963 中也包含有一个 ASN 值，该值意味着新的会话密钥从该 ASN 时刻开始生效。对于这个 ASN 值，网络管理器也必须要十分小心地选取一个合适值，以确保命令 963 能在该 ASN 之前被执行完毕。

1）如果命令 963 中的 ASN 是将来的，那么将会执行正常操作。

2）如果命令 963 中的 ASN 为 0 或 ASN 值丢失了，那么设备将立刻开始一个新的会话并使用这个新密钥。这主要针对新设备加入网络的情况。在入网过程中，新设备只要接收到入网响应，就立即转换到使用新密钥。

3）如果命令 963 中的 ASN 在当前 ASN 之前，那么设备将回复错误代码 0x42，丢弃该命令，并继续使用当前密钥。这也就是为什么网络管理器设定的 ASN 必须要足够的晚。

WirelessHART 网络设备在转换到使用新密钥之后，它应该继续保留着旧的密钥，以便处理后到达的旧报文。在最大报文寿命之后，旧密钥就可以被丢弃了。设备依据网络层头部中的 ASN 片段来确定是使用旧密钥还是使用新密钥。设备没必要同时尝试使用这两个密钥。

# 第9章　网 状 网 络

摘要：在这一章，我们将深入研究一些与网络相关的话题。这些话题归类为：设备生命周期、路由、上位机通信、网络管理、冗余、可扩展性、电池消耗、互操作性和非期望的访问。以下将每个话题列成一节标题。

## 9.1　WirelessHART 网络的诞生

当 WirelessHART 网关和网络管理器开始运行时，WirelessHART 网络便诞生了。当第一个 WirelessHART 接入点传输第一个通告报文的时候，WirelessHART 网络向外部世界宣告了它的存在。从技术上讲，网关会初始化一个通信来向网络管理器请求配置。因此，网络管理器是 WirelessHART 网络中第一个存在的设备。

实际上，WirelessHART 网络诞生于 ASN 为 0 的时刻，该时刻由第一个 WirelessHART 接入点确定，而第一个 WirelessHART 接入点设备是所有 WirelessHART 网络设备的时钟源。网络管理器、WirelessHART 网关和 WirelessHART 接入点间的通信不是无线的，可以是专有的通信协议。因此，第一个 WirelessHART 接入点什么时候设置其 ASN 为 0，这完全取决于供应商的实现。但是，网络管理器应该记录 ASN 为 0 对应的实际物理时间。

一旦第一个通告报文通过无线发送，WirelessHART 网络就存在了，其他网络设备即可开始加入网络。

ASN 值有 5 个字节，在不溢出的情况下能持续 3 个多世纪（>348 年）。

## 9.2　网络中设备的生命周期

对于 WirelessHART 设备而言，成功地加入网络是第一件、也可能是最困难的事情。WirelessHART 设备首先应该在所有物理信道上搜索通告报文，并实现与网络的同步。然后，它初始化入网过程。入网过程需要执行几次与网络管理器间的报文交互，这种报文交互需要通过代理设备来完成。在网络管理器完全配置新设备后，新设备就可以执行其在工业现场的职责了。

WirelessHART 标准定义了每层之间通信的 API，但是没有规定设备入网过程中的 API。对于新设备入网过程，每层之间的通信是协议栈内部的事情，可以有多种不同的实现方式。

接下来，我们将更详细地讨论每个步骤。从以下的内容，我们可以看到入网过程是如何被网络管理器完全控制的。网络管理器的好坏决定了设备是否能顺利地加入网络。

### 9.2.1 预配置新设备

加入密钥和网络 ID 必须被预配置给新设备。同一区域可能存在有多个 WirelessHART 网络。新设备需要网络 ID 以知道应该加入哪个网络。新设备也需要第一个密钥以加密最初的报文。最初的报文包含有将会被使用到的密钥的剩余部分。这些密钥的剩余部分必须在新设备和网络管理器之间被保护起来。命令 963（写会话）用于给配置加入密钥；命令 773（写网络 ID）能用于设置网络 ID。虽然这两个命令都是 WirelessHART 命令，但是它们也能通过 FSK 模块像有线 HART 命令一样发送给设备。

新设备也应当被设置成上电后自动开始加入网络。这个过程也可以通过命令 771（强制加入模式）来实现。

如何发布过程数据也可以被预配置给新设备。这个过程可以通过一系列常规命令（HCF_ SPEC-127）来实现。此外，如果新设备最后接收到了命令 109（突发模式控制），那么新设备在入网后就可以自动初始化过程数据的发布。

### 9.2.2 网络设备通告

WirelessHART 网络需要持续不断地发布通告报文。新设备利用该通告报文来实现与网络的同步，并从中提取出所有与入网相关的信息。WirelessHART 网络中的任何设备都能传送通告报文，以告知新设备如何通过其加入网络。通告报文包含了以下信息：

1）完整的当前 ASN 号。

2）4bit 的加入优先级，用来表征接收新设备的能力等级。该优先级的值是主要基于以下 4 个因素：到网关的跳数、信号强度、电池剩余量和后代的数量。优先级的值可以是这四种因素的权衡总和。

3）已用信道的信道图。

4）图路由 ID，被新设备用来发送报文给网络管理器。

5）超帧及其加入链路。对于发送通告报文的设备，如果超帧中的某个加入链路被设置成发送模式，那么该链路就应该被该设备专门用来发送数据，包括发送通告报文、给新设备的入网响应报文、向新设备写入超帧/链路以及在超帧/链路被配置之前的其他命令。对于发送通告报文的设备，如果超帧中的加入链路被设置成接收模式，那么该链路就应该被该设备专门用来接收数据，包括接收入网请求、入网响应报文的应答以及在超帧/链路被配置之前的其他命令。

通告报文允许在任何发送链路中传送。这样就可以减少新设备加入网络所花费的时间。

以上所有操作都是由网络管理器来配置和控制的。网络管理器采用命令 795（Write Timer Interval，写时间间隔）来向 WirelessHART 网络设备写入通告时间间隔。通告时间间隔值为 0 时，意味着尽可能快地发送通告报文；通告时间间隔值为 0xFFFFFFFF 时，则意味着停止发送通告报文。

在设备中，不是所有的超帧都包含有加入链路。然而，设备可以将没有加入链路的超帧放置于通告报文中。即使网络管理器没有分配任何加入链路给某个设备，但这也不能阻止该设备广播无加入链路的通告报文，因为 WirelessHART 标准并没有禁止这样的实现。

通告报文在数据链路层使用的是公共密钥，因为侦听这些通告报文的新设备并不知道网络密钥。

在“数据链路层规范”中的第 8.1.2 章节，WirelessHART 标准已经规定了网络 ID 的取值范围和目的。

### 9.2.3 新设备的同步

新设备将在某一个物理信道持续侦听一段时间，然后换到下一个信道，直到遍历完所有的信道或入网过程开始。新设备接收到一个通告报文，即可获知该 WirelessHART 网络所选用的信道名单，从而避开侦听黑名单所屏蔽的信道。

由于跳信道机制，新设备有可能在超时之前都无法侦听到一个通告报文。首先，通告报文可能永远无法在某一个选用的信道上传送。其次，当新设备在某个信道上尝试侦听通告报文时，而通告报文正好错过了此信道而在其他信道上被传送。在网络形成阶段，尽可能多的通告是很重要的，WirelessHART 接入点或有线供电的 WirelessHART 网络设备尤其应该尽可能地发送通告报文。

一旦新设备接收到了其所在网络的报文，并且该报文不是确认报文，那么该设备就可以设法与网络时间同步。由于确认报文的发送时间依赖于确认报文的长度，所以设备不可以通过确认报文来实现与网络的时间同步。

仅通告报文的信息会被新设备存储起来，而其他接收到的报文会被用来记录发送设备的邻居通信质量。

### 9.2.4 入网请求

一旦新设备接收到了通告报文，它就可以开始请求加入网络。新设备可以向多个设备发送入网请求。这时，新设备必须依据某种准则从中选择最好的候选设备。新设备通常选取信号强度最大的和加入优先级最高的设备，然后向其发送入网请求。其中信号强度比加入优先级更重要。

在响应模式中，入网请求报文的应用层载荷包含三个命令：命令0（报告邻居信号水平）、命令20（读长标签）和命令787（报告邻居信号水平）。这些命令都需要用入网密钥来加密，而报文中的安全控制字段会指明这些命令已被加密。因此，任何收到入网请求报文的设备都知道其是一个入网请求。它也被标明为图路由，而图路由ID是从通告报文中复制出的。数据链路层使用公共密钥来加密其载荷数据。

命令787包含了一个邻居设备列表，该列表中的邻居设备是新设备认为能很好为其提供入网服务的候选设备。收到入网请求报文的设备实际上会被认为是一个代理设备。入网请求报文将会在加入链路中被发送给代理设备。因此，代理设备的数据链路层识别出该入网请求报文，并将其向上递交给网络层。代理设备必须使用自己的路由路径来转发该入网请求报文，但是又不能修改用于加密的网络层头部。这也就是为什么新设备必须使用代理设备的图路由ID，同时代理设备必须有一个到达网络管理器的图路由路径。如果一个设备仅有源路由路径到达网络管理器，它一定不能发送通告报文来招揽想入网的新设备。

只要新设备的入网请求报文在数据链路层得到了确认，那么新设备就可以在需要时发送Keep-Alive报文来保持与网络的同步。在加入网络的初期，网络管理器可能还没有给新设备分配发送和接收链路，新设备这时可以占用加入链路来发送Keep-Alive报文。这些Keep-Alive报文也必须使用公共密钥来加密。

许多新设备可能同时竞争向某一个代理设备发出入网请求报文。于是，这些入网请求报文可能会相互冲突。因此，即使准备就绪，新设备也必须等待某个随机时间后才发送入网请求报文。该随机等待时间最多为2min。

### 9.2.5 入网响应

网络管理器应该预先知道新设备所使用的入网密钥，因为它需要使用该密钥来认证新设备发出的报文。网络管理器也可能预先知道新设备的ID。这样，其他拥有不同ID的设备将不允许加入网络。设备的长地址可以从命令0的响应报文构造出来。网络管理器将构造出的长地址与报文等层头部中的长地址相比较，从而也可以检查出入网请求报文的合法性。

一旦新设备入网被认证通过，网络管理器就将返回一个入网响应报文。入网响应报文包含三种命令：命令961（写网络密钥）、命令962（写设备昵称地址）和命令963（写会话）。入网响应报文实际上不是一个响应命令，而是一个请求命令。新设备需要返回其对应的响应。

代理设备负责路由入网响应报文。网络管理器从入网请求命令787中选取其中的某个设备，然后用该设备作为代理设备来构建入网响应报文的路由路径。入网响应报文会被路由给代理设备，就好像该代理设备是其最终的目的地一样。代理设备

会检测到请求响应报文中的代理标志位，然后利用自己的加入链路时隙转发该请求响应报文给对应的新设备。

网络管理器为入网请求响应选取的代理设备可能与新设备发送入网请求报文的代理设备不同。毕竟，对于网络管理器来说，它甚至并不知道哪个设备发送了入网请求。

在命令787中列出的所有邻居设备的所有加入链路所对应的时隙里，新设备都应该保持活跃状态。新设备可以从入网响应报文中获得分配给自己的短地址，并从此开始使用该短地址。新设备甚至在回复入网响应报文的时候也将使用该短地址。

除了与手持设备相关的报文外，长地址仅用于入网请求报文和入网响应报文。

新设备也应该立即使用密钥。对于入网响应的回复报文，新设备在数据链路层使用网络密钥对整个报文进行加密，同时在网络层使用命令963提供的单播会话密钥来加密回复报文的内容。当入网会话结束时，入网密钥就不再被使用了，直到下次入网会话时才会被再次使用。

入网响应报文属于入网会话，而对入网响应报文的回复属于单播会话。因此，网络管理器必须继续使用单播会话中的入网会话序列号。

至此，新设备已经成功入网了。密钥、超帧和链路配置命令必须被转发给新设备的应用层，然后新设备的应用层再返还给自己的网络层。网络层不知道入网过程是否完成，直到应用层告知它。

在加入链路上侦听的设备应该准备使用公共密钥或网络密钥来处理接收到的报文。当代理设备在加入链路上接收到一个报文的时候，该报文可能是公共密钥加密过的入网请求或者是网络密钥加密过的写超帧/链路命令。这也就是为什么DLPDU标识符中的密钥标志位很重要。DLPDU标识符中的密钥标志位指明了报文中使用的是哪种密钥。然而，在大多数情况下，接收方也可以利用其他相关信息猜测出报文中使用的是哪种密钥。

### 9.2.6 更多的配置

1. 写超帧和链路

新设备被分配了普通链路之后，就不再需要使用加入链路进行通信了，也不再需要代理路由。新设备与代理设备之间的代理关系也就此终止了。事实上，代理路由存在的时间是在入网请求之后，普通链路被分配之前。新设备一旦接收到一个单播发送链路，就将停止使用入网发送链路。同样的，新设备一旦接收到一个单播接收链路，就将停止使用入网接收链路。这两种链路都被分配给新设备后，新设备也将移除从通告报文中获得的超帧，除非网络管理器又重新配置了这些超帧。入网响应报文之后的第一个报文建议被用来写超帧和链路，该报文也是除了入网响应报文外唯一由代理设备路由的报文。对于设备到网络管理器的上行路线，仅入网请求报

文和入网响应的应答报文是由专门的代理设备负责路由的。网络管理器依据入网请求报文中提供的邻居表给新设备分配通信链路，也可将其他网络设备配置为新设备的邻居设备。代理设备并不一定是新设备唯一的邻居设备。在一些特殊案例中，新设备和代理设备之间可能没有被分配任何通信链路。

2. 写到网络管理器的路由路径

在新设备与网络管理器之间的路由路径被配置好之前，新设备会构建一个默认的图路由。该图路由的 ID 是从相应的通告报文中获得而来的，新设备的代理设备是该图路由的转发邻居设备。一旦网络管理器为新设备分配了路由路径，那么默认的图路由就必须被移除。

3. 写时间参数

网络管理器也必须使用命令 971（写邻居性能标志）来为新设备配置时钟源。该时钟源有可能并不是新设备的代理设备。为了让新设备能将数据或事件标上时间戳，网络管理器也应该使用命令 793（写 UTC 时间映射）来向新设备写入全局时间。

4. 写网关会话和路由

虽然网络管理器控制着整个 WirelessHART 网络，但是网络管理器需要通过网关来履行职责。新设备拥有了与网关的会话、到达网关的路由路径和图信息，这才意味着该设备完全加入网络了。

### 9.2.7 在网状态的维持

新设备加入网络后，还必须采取一些行动来维持其在网状态。设备在网状态的维持可以通过时间同步来实现。每次报文交换就能实现一次时间同步。所有网络设备将各自的邻居设备健康信息发送给网络管理器。网络管理器依据这些信息来不断地调整网络，这样也能维持设备的在网状态。

出于安全考虑，网络管理器还需要周期性地更换密钥。同时，入网密钥也可以被更换，被更换后的入网密钥在下次入网时才生效。

### 9.2.8 断开网络

在网络运行期间，设备有时候必须从网络中断开。设备、网络管理器或手持设备都能初始化断开过程。网络管理器可以向设备发送一个断开网络命令——命令 960。或者，设备可以通过向所有与自己有链路关系的邻居设备发送一个数据链路层断开报文，从而自主地从网络中断开。断开报文在数据链路层内就被完全处理掉了，不需要提交给上层处理。然后，邻居设备将这一消息通过健康报告的形式间接地告诉给网络管理器。该设备也可能突然失效，对于这种情况，该设备的邻居设备将向网络管理器报告与该设备失去了联系，网络管理器据此推断出该设备已经从网

络中断开了。

### 9.2.9 重新加入网络

设备一旦失去了时间同步，就不得不重新加入网络。WirelessHART 标准的早期版本 7.0 提供了一种 Re-Syching 状态。设备在该状态时能保存全部的配置信息，并可以快速地回到网络。为了简化，该状态后来在后期版本的 WirelessHART 标准中被删除掉了。所以，设备一旦失去了时间同步，其全部的配置信息将被去除，WirelessHART 网络也认为该设备已经死亡。该设备应该努力重新加入网络，就好像这是第一次加入网络。

## 9.3 路由

WirelessHART 网络将承担源节点到汇聚节点的数据中转，即路由。数据的路由方式有许多种，每种方式适合不同的用途。WirelessHART 网络路由的目标是准时、可靠地传递数据。WirelessHART 提供了源路由（Source Routing）、图路由（Graph Routing）和超帧路由（Superframe Routing）。当新设备入网时，代理路由（Proxy Routing）也会被使用到。

源节点和汇聚节点之间要建立起会话才谈得上中间路由这一概念。虽然 WirelessHART 标准支持两个现场设备之间的会话，但是实际上所有的会话都位于现场设备与网络管理器或网关之间的。在本小节，我们仅讨论现场设备与网关之间的路由。网络管理器一直都是通过网关来与现场设备通信。我们也会用到术语“up”和“down”，例如“up”链路和“up”路由被用来描述现场设备到达网关的路径、“down”链路和“down”路由被用来描述网关到达现场设备的路径。

### 9.3.1 源路由

源路由是简单易懂的。源路由设备在其报文中包含了整个路由路径，每个中间设备只需简单地将该报文转送至路径上的下一个设备。网络管理器和网关常常使用源路由，因为它们知道网络拓扑结构从而能构建出完整的路由路径。如果某个现场设备想使用源路由，那么网络管理器必须对该现场设备进行配置，网络管理器可以使用命令 976（写源路由）来向该现场设备写入整个路由路径。该路由路径也将被过命令 974（写路由）被告知与其对应的目标设备地址。设备根据目标设备的地址来查找路由路径。如果该路径被配置为源路由，数据报将会按照源路由的方式路由。

### 9.3.2 图路由

对于图路由，设备依据报文中2个字节的图ID来传递报文。一个图ID代表着一个方向图，该方向图的顶点是设备，该方向图的方向边是发送方到接收方的传输链路。图由网络管理器来构建。在图路径上的每个设备都必须接收到图ID信息，并获知图路径中输出边对应的每个邻居设备的地址。设备应该选择第一个可用的并且对应着图的一个路由边的链路来转发报文，不管该链路是连到哪个邻居设备。图路径中的任何设备，如果它也在该图路径上发送自己的数据，都必须知道图路径对应的目标设备地址。

显然，为了工作正常，图中的所有路径都必须指向单个目标设备。网络管理器的职责之一就是构建正确的图。显然，图中也应该不存在环路以避免报文无休止地在环路中传递。没有环路的图路由能保证任何报文的及时传递。然而，WirelessHART标准并没有禁止图中的环路。例如，如图9-1所示，4个设备（A、B、C、D）组成了一个5条边的图。设备B能发送报文给设备C或设备D。设备A发出的报文中会嵌入有一个图ID，并通过设备B或设备C路由至目标设备D，或者依次通过设备B和设备C路由至目标设备D。

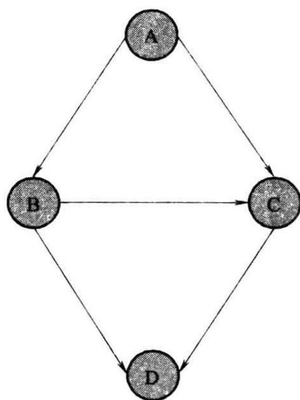


图9-1 图路由

因为WirelessHART网关是唯一的汇聚节点，所以它到每个现场设备的“down图”都是不相同的。所有现场设备可以共享一个到达网关的“up图”。此外，这个共享的“up图”也可以被用来路由报文给网络管理器。

### 9.3.3 混合路由

网络层头部中的不同字段分别定义了源路由和图路由信息，并且源路由和图路由信息可以共存于一个报文中。这样可为报文的路由提供更好的灵活性，并且路由成功的几率更大。如果一种路由方式失效，那么路由设备还可以选择另外一种路由方式。此外，一些特别的规则也可促进报文的传输。例如，如果目标设备是其邻居设备，设备可忽略路由指令，而直接向该邻居设备发送报文。接下来的问题是：我们愿意选择弱信号强度的一跳而直接到达接入点，还是选择强信号强度的多跳路由？所有特别的规则都总结在“网络层规范”[⊖]的9.3.3.2节和表19（数据报的路

⊖ 相关规范的名称和编号见参考文献，读者可自行查找。——译者注

由）中。

### 9.3.4 超帧路由

WirelessHART 标准还包含了图路由的一种特殊形式，即超帧路由。在超帧路由中，设备根据报文中的超帧 ID 转发报文。网络管理器负责超帧的创建。与超帧中任何链路相关的任何设备都必须接收该超帧和链路信息。不管其邻居设备是哪个，设备都应该选择超帧中第一个可用普通发送链路（Normal Transmit Link）来转发报文。如果设备使用超帧路由来发送数据，那么该设备也必须知道目标设备对应的超帧路由，从而进一步知道该超帧路由对应的超帧。

为了不改变报文格式，WirelessHART 标准决定使用报文中的图 ID 作为超帧 ID。如果该字段的值小于 255，那么其是超帧路由 ID；如果该字段的值等于或大于 255，那么它就是图路由 ID。因此，一个有效的图 ID 一定都大于 255。

例如，对于图 9-1 中的 4 个设备，如果我们打算使用超帧路由，那么我们可以创建一个仅有 5 种设备间链路的超帧：设备 A 到设备 B 的链路、设备 A 到设备 C 的链路、设备 B 到设备 C 的链路、设备 B 到设备 D 的链路、设备 C 到设备 D 的链路。

1. 图路由转换成超帧路由

图 9-1 的案例在一定程度上显示了图路由和超帧路由的等价。对于任何图路由，我们可将其转换成超帧路由。

我们可定义一个所有链路都是普通链路的超帧。该普通链路是由图 9-1 中的有向边对应转换而来的。链路的发送方对应着有向边的起始端，而链路的接收方对应着有向边的终止端。从拓扑上讲，这种转换保存了报文传输过程中所有可能的路径。

然而，由于可用链路数量的差异，这样推导出的超帧路由无法与正在使用中的图路由完全匹配。对于图路由，任何超帧中的任何链路都可被使用。而对于超帧路由，仅超帧路由对应的超帧中的链路可被用来转发报文。我们可以估计图中每条边将占用多少链路，然后在超帧中定义同样数量的链路。然而，图路由需要与其他数据通信竞争这些链路，而超帧路由则不需要。

2. 超帧路由转换成图路由

同样的，我们也可以将超帧路由转换成图路由。以下描述了如何从超帧路由创建出图路由。图 9-1 中的众多顶点代表着一系列的设备，每个设备在超帧中有至少一个相关的普通链路。对于超帧中的每个普通链路，我们都可在图中构建一个从发送方到接收方的有向边。我们可以保留该超帧，这样该超帧的全部普通链路能被用于新的图路由。或者，我们可以移除该超帧，然后为新的图路由定义另一个超帧以为其提供链路。

同样的，从网络拓扑结构上讲，这种转换保存了报文传输过程中所有可能的路径，但是运行期间的行为无法完全一样。

3. 比较

从网络拓扑结构上讲，图路由和超帧路由是一样的。但是，它们也有着一些细微的差别。

1）图路由已得到了广泛的研究，并且易于理解。

2）超帧路由在数据传输的隔离性方面更好，即在网络中数据传输受其他通信的影响较少。超帧路由在保证实时性方面更好。

3）超帧路由会占用更多的设备资源。然而，设备能够配置的超帧总数有限。因此设备无法承担太多超帧路由。同时，当超帧数量过多时，设备还不得不花费更多的计算来从超帧中找出当前的链路。

4）超帧路由和图路由都需要网络管理器的精心管理。对于这两种路由方式，一个差的网络管理器可能会导致无终止的环路、死胡同，或数据报无法到达的目的地。

5）超帧路由仅仅使用本超帧中的链路，而源路由和图路由能使用任何超帧中的链路。当多种路由方式同时存在的时候，这三种路由方式会竞争所有的链路。这时，图路由和源路由将会更有优势，因为它们可以比超帧路由抢占到更多的链路。

如果超帧路由是网络中唯一的路由方式，那么所有的数据通信都将有专用的链路。这些专用的链路将不会被其他数据通信占用。那么，端到端的数据传输延迟就有保证，且能被计算出来。此外，如果路由路径有冗余路径，那么就能较好地防范单跳通信失败。

### 9.3.5 代理路由

如9.2.4节所述，代理设备必须将其“up”图ID置于其通告报文中。新设备在被分配了属于自己的路由之前，都必须使用该图路由ID来构建报文。之前，我们简单地提到过代理路由。现在，我们将更详细地讨论代理路由。

像源路由和图路由一样，代理路由在报文的网络层头部也有其自己的字段。发送给新设备的报文会按照图路由或源路由的方式路由给代理路由设备，就好像该报文的目标地址是代理设备一样。换句话说，发送方对这些路由字段的设置就像它正在发送一个普通报文给代理设备。如果发送给新设备的报文采用源路由的方式来传递，那么源路由列表中的最后一个地址应该是代理设备；如果发送给新设备的报文采用图路由的方式来传递，那么图ID应该是网络管理器到代理设备的“down”图。只有代理设备能处理报文中的代理字段。代理设备最后会将该报文转发给新设备。对于代理设备转发给新设备的报文，其网络层头部中的目标地址将是新设备的长地址。代理路由对中间路由设备的影响是它们在自己的邻居列表中找不到这个新

设备。

### 9.3.6 广播路由

“网络层规范（HCF_ SPEC-85）”中的表19制定了一些如何路由报文的规则。这里将介绍网络管理器或网关如何广播报文，即广播路由。

形成广播图：广播图是单向的图，它有一个源节点。广播图中，从源节点到任何节点至少有一条路径。为了图的冗余，每个设备至少有两个接收链路。唯一的源节点会产生广播报文。该广播报文沿着图的所有边流动。图中的每个节点都将接收、处理和转发该广播报文。图的链路将被定义到超帧中。广播图最简单的构造方法是对共享的用于上传数据到广播源节点的图路由中所有的边进行反向。

配置广播树：网络管理器发送图信息（如超帧）给图相关的设备。链路的属性将被设置为广播类型。

形成广播报文：网络管理器或网关在网络层头部和数据链路层头部中都将报文类型设置为广播报文。换句话说，报文中的目标地址被设置为0xFFFF。网络层头部的图ID将是超帧ID。

转发广播报文：现场设备在其广播接收链路上接收到广播报文后，它将像接收者一样来处理该报文，并在其广播发送链路上广播该报文。如果广播报文中的图ID不是超帧ID，那么现场设备可以选取任何超帧中的广播链路来广播该报文，已公布的“网络层规范”并没有清楚地描述这一点。

## 9.4 WirelessHART网关与上位机的通信

对于WirelessHART网关与上位机之间的连接，WirelessHART标准并没有规定使用什么样的通信介质。因此，任何网络都可以考虑被用于WirelessHART网关和上位机之间的连接，如以太网、因特网、Wi-Fi、Fieldbuss等。更高层面的XML语法也可用于这些网络间的信息交互。因为WirelessHART标准是基于有线HART的，所以其最大的优势是上位机不需要使用一个全新的应用层解决方案，而只需要简单地使用HART解决方案。这样，底层网络所需要做的就只是传递HART命令和响应。

对于网关与上位机之间的连接，我们可以使用已有的线缆或无线骨干网络，而不需要布置新的线缆。接下来，我们叙述一个使用已有Fieldbus网络的解决方案。

为了允许WirelessHART设备被简单、低成本地整合到已有控制的系统中，其他现场总线设备可被设计成具有WirelessHART网关的功能。这些具有网关功能的现场设备将被设计成可将WirelessHART协议转换成Foundation Fieldbus™（FF）或Profibus DP协议。这样，这些现场安装的、具有网关功能的现场设备就可以通过有

线连接到大多数现代控制系统支持的 FF 和 Profibus fieldbus 接口。这种方法将允许低廉的网关被安装在现场，并靠近一个处理单元中的无线发送器。这类网关设备还能从现场总线获得电源。如果采用这种方案，支持 FF 或 Profibus Fieldbus 接口的控制系统就能很容易地与这类网关设备相连。这样，WirelessHART 设备就能被简单、快速地安装到这些控制系统中。

总的设想是，这类现场安装的网关设备能像传感器或类似现场设备一样，组装在粗壮紧凑的外盒中，由总线段供电，并安装在靠近无线设备群的现场中。这些无线网关将被设计成既包含 FF 或 Profibus 标准使用的协议栈，又包含 WirelessHART 标准协议栈。FF 或 Profibus 应用层将担当这两种标准间的粘胶剂，例如 WirelessHART 协议栈中的通信参数将被映射为功能块应用的标准参数。

## 9.5 网络管理

网络管理器是 WirelessHART 网络的核心。网络管理器的好坏能显著地引起 WirelessHART 网络性能的变化。本小节将列出一些与管理网络相关的关键点。

### 9.5.1 设置超帧长度

通信链路能被组建成各种超帧，如维护超帧、突发数据超帧、入网超帧等。如果不同超帧中的链路在同一个时隙相互冲突，那么问题就发生了。WirelessHART 标准允许这种问题存在，并采用优先级的方式来解决该问题。当然，更好的情况是根本不发生这种问题。网络管理器应该精确地统筹链路。为了检查时隙是否相冲突，网络管理器可以在所有超帧长度的最小公倍数内逐个检查每个时隙。我们知道在最小公倍数之后一切开始重复。

一个更简单的方法是从“harmonic”链（Kuo and Mok 1991）中选择超帧大小。“harmonic”链是一列数。除了第一个数，该列表中的每个数都是前一个数的倍数。如果 $x$ 和 $y$ 是“harmonic”链中的两个数，那么 $x$ 可以整除 $y$ 或 $y$ 可以整除 $x$。由于超帧大小都是选取于“harmonic”链，那么任何小的超帧将在大的超帧范围内重复。这样就能更容易的调度出两个没有链路冲突的超帧。例如，调度器可以从最短超帧开始调度；然后，调度器开始调度下一个最短超帧，并避免分配任何更短超帧中已占用的时隙；调度器重复使用这种方法调度下一个最短超帧，直到最后调度最大的超帧。

实际上，我们也能够依据表达式 $ab^n$ 来分配超帧大小。在表达式 $ab^n$ 中，$a$ 和 $b$ 是两个常数，$n$ 是任何一个自然数。序列 $ab^0$，$ab^1$，$ab^2$，$ab^3$，……可以被证明是一个“harmonic”链。

超帧大小也应该首先考虑到选用的信道数，这样超帧中的链路就有可能使用到

所有的物理信道。如果超帧大小是可用信道的倍数，那么超帧中的某个链路将总会使用同一物理信道。

### 9.5.2　为上位机分配带宽

从本质上讲，WirelessHART 网络的目标是支持上位机。从根本上说，这意味着 WirelessHART 网络设备将感知测量数据，并将这些测量数据发送给上位机、同时还要处理来自控制应用程序的请求。网络管理器应该为这些数据传输分配相应的通信带宽。

对于一个已配置的上位机控制策略，用于传输测量数据的链路是这样调度的：当与设备相关的控制策略被下载到设备时，例如告诉设备报告什么样的突发数据以及多快地报告突发数据，设备将向为其创建链路的网络管理器发送请求。WirelessHART 标准并没有定义如何请求链路来发送控制数据给执行器。应该有一种定制的方式使得网络管理器能将控制策略转换成针对执行器数据的超帧链路。

入网过程中的隔离阶段可以被用来做很多事情：在 WirelessHART 网络启动期间，所有的设备都处于隔离阶段；接着，网络管理器下载控制模块和产生调度信息；然后，调度信息被发送给设备，从而让设备进入运行状态。此外，如果 WirelessHART 网络处于运行状态，我们只需要关闭 WirelessHART 网络中所有的数据超帧，就能使 WirelessHART 网络进入这样的隔离状态。于是，我们就可以做任何维护网络的工作和产生新的调度，然后再通过使能它们的数据超帧就可以让新设备重新恢复到运行状态。

### 9.5.3　一些注解

以下是一些与网络管理功能相关的注解：

1）WirelessHART 标准没有定义添加邻居（ADD_ NEIGHBOR）命令和删除邻居（DELETE_ NEIGHBOR）命令，它们是固有的内部功能。设备必须根据通信情况和网络管理器对它的配置来维护自己的邻居信息。

2）为了减少多跳路径中的传输延时，网络管理器可以设法将超帧中的一段连续时隙依序分配给多跳路径，这样就可以将路径上的链路级联起来。这种方法的一个局限是链路可能会被其他数据通信占用。

3）网络管理器通过网关来控制网络。一个网络管理器应用进程可能控制着多个 WirelessHART 网络。

4）网络管理器对整个 WirelessHART 网络的调度应该逐渐地适应网络的变化，以最大可能地避免对现有通信的破坏。调度的优化也应该是个渐进的过程。WirelessHART 标准工作组在标准制定之初就有一个约定：网络管理器应该偶尔全局性地优化整个网络的调度，以梳理当前网络的拓扑结构和应用。网络梳理的评判准则

可以是载荷的均衡、能量感知、时间尺度等。

5）WirelessHART网络本身是一种资源，也是整个过程工厂的资产。网络管理器应该代表着一种可被以下应用进程访问的网络：网络健康趋势、网络故障诊断与维修、网络健康警报等。

## 9.6　冗余

冗余在过程自动化中一直都是很重要的。一些用户将冗余作为任何控制系统的先决条件。WirelessHART标准也完全意识到了冗余的重要性，并对此提供了足够的支持。冗余能允许系统在发生某些失效的情况下还能保持运行。保持运行在过程控制系统中是至关重要的。最常见的冗余是双冗余，用以防范单个失效。换句话说，如果双冗余设备同时发生失效，系统可能也失效了。为了防范单个失效，系统中的每个部分都应该分别有一个处于待命状态的替代者。

### 9.6.1　设备冗余

在WirelessHART网络中，网络管理器、网关、或任何现场设备都有可能失效。

网络管理器：每个WirelessHART网络只有一个网络管理器。为了提供冗余，备用网络管理器应该与处于工作状态的网络管理器保持同步。当处于工作状态的网络管理器被强制关闭或失效时，备用网络管理器将接替其工作。替换的协调由具体实现决定。

网关：每个WirelessHART网络也只有一个WirelessHART网关。备用网关可以被用来提供冗余。备用网关通常应该保持于非工作状态。除非当处于工作状态的网关失效或被命令要求切换时，备用网关才会进入工作状态。备用网关与工作网关之间的协调由开发者自己决定。

接入点：虽然供应商能够布置备用接入点来实现对接入点的冗余，但是在WirelessHART标准中接入点的冗余是通过多个独立接入点来实现的。每个独立的接入点与网关之间都有自己的直接联系，并在网络中都有着自己的短地址。如果某个接入点失效了，那么数据将被自动地路由到其他的接入点。

现场设备：冗余现场设备的概念超出了WirelessHART标准的范围（实际上，冗余测量常被用于关键回路）。如果两个设备采集到相同的数据，那么它们将被看成是网络中两个完全不同的设备，就像接入点的冗余一样。然而，如果某个现场设备还承担路由功能，那么它的失效就会影响到网络中的其他设备。这时就需要使用路由冗余。下一个章节将讨论路由冗余。我们能够使用其他现场设备作为替代路由器。增强网状网络健壮性的一个有效方式是布置一些额外的设备，让它们在网络中担当路由器的角色。

### 9.6.2　路由冗余

报文中的源路由只提供了单条路径，而没有提供冗余路径。如果路径上的某一跳失效了，报文就将丢失。为了提供冗余，源节点应该在超时后尝试使用另外一条不同的源路由路径来重新发送该报文。接下来，我们重点关注图路由的冗余。除了汇聚节点，如果其他节点都至少有两个可转发报文的邻居节点，那么单次通信失效就能被克服。

#### 9.6.2.1　问题

使用有向图，自然会有一个到汇集点的连接是非冗余的。单方向性被用来避免循环。为了提供冗余，每个节点要求拥有多个链路来转发报文。然而，就汇集点之前的节点而言，如果在图路径上不创建一个循环，那么该节点就不能提供全冗余。因此，对于从某个节点发送给汇聚节点的数据而言，全冗余是不可用的。如果某条没有冗余的链路失效了，那么设备就不知道该向谁发送报文了，这样报文也就丢失了。下图9-2描述了这个问题的一个案例。值得注意的是：不管网络中有多少个接入点，要避免循环，网络中至少有一个接入点与网关之间仅有一条连接。

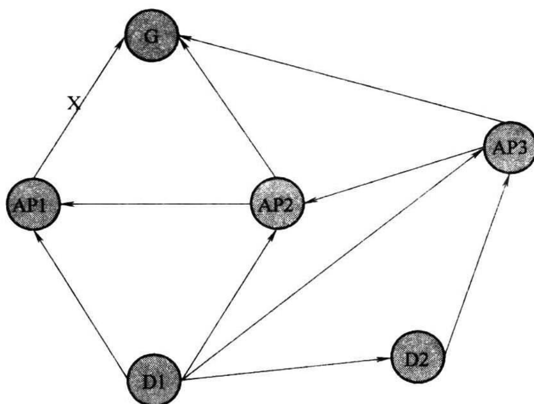



图9-2　图路由中的单跳失效

调度的随机性导致每条被发出的报文可能经历不同的路由路径。这样的好处是，如果上述问题造成报文丢失，它只会减少数据更新率，而不会造成完全失去对工业过程的观察。然而，调度的非确定性属性不能保证更新率到底能降低多少。一旦网络管理器意识到了链路失败，那么它就可以找出问题并采取纠正措施。

对通向网关的图，该问题就非常小并且能通过增加更多的硬件设备来解决。网关可以通过有线网络与每个接入点直接通信。这样做的一个好处是：网关和接入点之间有线连接产生中断的概率远低于无线连接产生中断的概率。另一个好处是：网

络管理器能够立即意识到故障的发生，这样网络管理器就能提高警觉并迅速采取纠正措施。如果在网关和接入点之间增加有线冗余网络，那么网关和接入点之间通信中断的情况就可以被避免。当然，如果 WirelessHART 网络只有一个接入点，那么网络中将会存在一个非接入点（NAP）设备，该设备仅有一个最后一跳连接到接入点。对于拥有多个接入点的 WirelessHART 网络，我们也可以证明：除非某个节点能与多个接入点直接通信，否则我们将面临同样的问题。

上述问题同样存在于通向设备的图路由。当至少一个节点与汇聚节点之间只存在有一条链路时，同样的瓶颈问题也会发生。网络管理器由于距离问题可能要过几分钟才意识到这个链路失败。由于发送给设备的数据可以影响过程控制，所以这些数据也被认为是很重要的。一个办法是通向设备的数据由冗余源路由路径来传输。

值得注意的是这里所有的讨论都是假设网络管理器总是产生最佳方案。它所产生的图中只有不可避免地到汇集点的最后一个非冗余节点。这进一步意味着，至少有另一节点能转发报文到此非冗余节点和汇集点。

上段最后一句话可以被证明。此外，我们可以证明，要保证除了非冗余节点之外的冗余，至少有一个节点应该直接连接到两个不同的接入点。

然而，WirelessHART 标准明确禁止图路由路径中存在环路。网络管理器调度生成图路由路径。网络管理器的具体实现由系统供应商完成。如果图路由路径中存在环路，那么数据报可能会无休止地循环从而无法到达目的地。WirelessHART 标准还定义了数据报的生存时间，这样数据报就不会被永远循环传递；相反，它会在循环了一段时间后被丢弃掉，但是这样还是会浪费带宽和能耗。

WirelessHART 标准还定义了路由规则。以下规则对于后续讨论很重要。该规则引用自 HCF_ SPEC-85 中第 9.3.3.2 小节：“如果单播 NPDU 的目标地址与邻居节点的地址相匹配，那么该 NPDU 必须被直接发送给该邻居设备……。如果这次发送失败了……，那么该数据报必须通过图路由的方式来传输（如果可能的话）。”

上述规则能够减轻单个非冗余节点问题造成的影响：如果某个节点同时拥有汇聚节点和单纯节点作为其邻居转发节点，遵循上述规则，该节点将会首先尝试向汇聚节点转发数据报。因此，途径该节点的任何数据报都被提供了单次故障保护。当非冗余节点和汇聚节点之间的连接失效时，仅有从其他路径路由给该非冗余节点的数据报会丢失。一个好的网络管理器能够构建相应的图路径来避免这种情况的发生。

#### 9.6.2.2 一个可能的解决方案

如图 9-3 所示，图路径是一系列实心箭头线。节点 B 和节点 C 分别是目标节点 D 的两个直接邻居节点。节点 B 的替代路径经过节点 C，但是节点 C 没有替代路径到目标节点。我们可以在图中加上节点 C 到节点 B 的箭头点线。如果目标节点是自己的邻居节点，那么该节点将一直尝试向该目标节点发送报文，这是符合

WirelessHART 标准规定的。然而，如果节点 C 到节点 B 的链路不存在，那么上述问题就无法得到有效的解决。

针对该问题的解决方案需要网络管理器和特殊节点的协调。首先，网络管理器试着在目标节点与其邻居节点之间添加直接链路以构建冗余。相邻节点间的环路是允许的。如果这样做不到，网络管理器可以从非冗余节点加条链路到特殊节点。在图 9-3 中，特殊节点将是节点 A，新链路将是节点 C 到节点 A 的箭头点线。如果节点 C 到节点 D 的链路发生错误，报文将被转发回节点 A，然后再转发给节点 B 和节点 D。

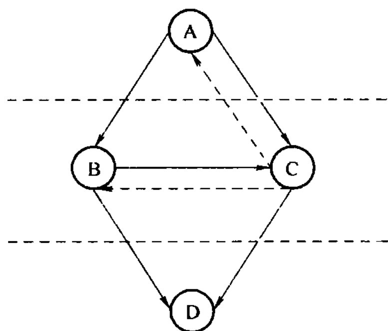



图 9-3 冗余图

该特殊节点需要实现一点：该特殊节点会记录下途径该特殊节点的报文和该特殊节点发送给邻居节点的报文。这种特色在许多路由机制中是普遍存在的，在 WirelessHART 设备中实现也不难。

现在，我们来分析一个实例。如果报文被路由给节点 A，节点 A 随机地转发该报文给节点 C。然而，节点 C 到节点 D 的链路失效了。因此，节点 C 会返回该报文给节点 A。节点 A 记得该报文，因而节点 A 将该报文重新转发给节点 B。即使节点 B 与节点 C 的链路存在，节点 B 将不会转发该报文给节点 C，因为节点 D 是其直接邻居节点。因此，该报文从节点 A 传输至节点 D 花费了 4 跳。

通过利用特殊节点，网络管理器能产生完全冗余的图，甚至可以为报文提供可确定的最大延迟。网络管理器必须小心地创建图以避免无终止的报文环路。一旦创建了图，网络管理器也能计算出报文从源节点到目标节点的最大跳数。这种想法能够被推广使用到更复杂的案例。只要图中的环路能被特殊节点断开，并且报文的跳数可确定，那么图就能被部署。例如，向后的链路未必来源于目标节点的直接邻居。这种情况是有可能发生的，例如，假如图 9-3 中的节点 A 没有链路可到达节点 B，或可到达节点 D 的任何其他直接邻居。于是，节点 A 也必须有一个向后的链路到达其他节点以建立一条到达节点 D 的冗余路径。

"up graph" 是用于从现场设备到网关的数据路由。即使现场设备通过接入点连接到网络，并且接入点之间被假设为完全互联，上述讨论的问题也可应用于 "up graph"。例如，如果某个接入点的每个直接邻居仅能与一个接入点通信，那么这些节点将面临同样的情况，它们之间必须创建一个环路以提供冗余路径。

特殊节点不需要永远记住以前的报文。特殊节点可以将每个报文与报文对应的生存时间联系起来。一旦报文的生存时间结束，特殊节点就可将该报文从其记录列表中删除。根据 WirelessHART 标准的规定，如果某个报文的生存时间结束了，但

是其仍然在路由路径上，那么路由节点必须丢弃该报文。因此，特殊节点不必担心报文是否会在其生命周期后被返还回来。

#### 9.6.2.3 一个替代解决方案

通过进一步增强特殊节点的功能，我们能为网络管理器提供更多的控制力。如果特殊节点的所有可转发报文的邻居节点都失效了，那么特殊节点将返还报文。这就是特殊节点的另外一个特色。例如，如果图9-3中的节点A和节点C都是增强型特殊节点，那么我们甚至不必添加从节点C到节点A的链路。节点C将返还报文给节点A，然后节点A将重新发送该报文给节点B。这使得网络管理器在创建图方面获得了更多能力。当然，网络管理器也应该更小心地处理。

利用增强型特殊节点，我们可以定义非常简单的图（graph）以提供确定性冗余路由。例如，一个图能包含两条从源节点到目标节点的独立路径。这两条路径上的每个节点都可作为增强型特殊节点。如果任何一条链路失效了，报文将会被原路返回给源节点，而源节点只需要在另外一条路径上重新发送。

同样的，这种特色在许多路由机制中也是普遍存在的，在WirelessHART设备中实现也不难。这些特殊节点也可被选择性地增强，从而能够选择邻居节点来转发报文。例如，特殊节点可再次选择上次通信成功的邻居设备，从而避免选择上次通信出现问题的邻居设备。

### 9.6.3 广播冗余

广播报文的不同之处在于其有多个接收方，并且这些接收方在数据链路层都不会确认收到报文。因此，发送方无法得知哪个接收方已经成功地接收到了广播报文。这也就是为什么一个节点必须有两个广播源。如果该节点没有接收到其中一个广播源发出的广播报文，那么它还能从另一个广播源获取广播报文。我们可以在超帧中通过创建链路来建立广播路径。例如，网络管理器将一个链路分配给一个广播报文发送方，同时将该链路分配给多个广播报文接收方。

## 9.7 可扩展性

WirelessHART网络是小规模、低数据率、低功耗的网络。当发送功率为10dBm时，非直视接收距离理论上为75m，而直视接收距离为200m。一个典型的过程工业车间大约为足球场大小，即长大约为100m、宽大约为50m。对于覆盖区域而言，一个WirelessHART网络在不需要多跳的情况下能够覆盖整个车间。

在小节8.1.1中我们计算出，WirelessHART网络的最大过程数据接收率是每秒钟1.5千数据条目，即每秒钟31.5k~55.5k数据字节。通常，一个传感器提供一到四个测量数据，一个驱动器操作于控制环路的另一边。WirelessHART标准允

许传感器的最快采样时间是 0.25 s。由于 WirelessHART 网络的最大过程数据接收率是每秒钟 1.5 千数据条目。因此，WirelessHART 网络能够最多承担大约 400 个快速采样的设备。假设 WirelessHART 网络的占有率为 40%，我们仍将有 160 个设备。

一个工厂车间内可能布置有多个 WirelessHART 网络。每个 WirelessHART 网络有几十个节点，并且位于一个独立控制单元周围。所有这些小型的 WirelessHART 网络可以形成一个簇，并由控制室中的上位机控制。

## 9.8 低功耗模式和电池寿命

WirelessHART 设备通常是由电池供电的。电池的预期寿命（McCluer 2003）是很重要的。为了节省能量，WirelessHART 设备在没有通信需求时被允许进入低功耗模式。网络管理器可以通过配置设备中的链路，使得其在一段周期性的时间内没有活跃链路。那么，设备就可以在这段时间内关闭射频部分的电源并冻结操作，甚至可以进入睡眠状态。然而，由于 Keep-alive 的时间间隔是有限的，所以设备的睡眠时间不能超过 Keep-alive 的时间间隔。

mA · h（Milliampere-Hour，毫安培小时）是一个典型的电池容量单位，即如果电流是 1A 时可用多少小时。电功率等于电压乘以电流，能量等于功率乘以时间。因此，能量单位应该是电压 × 电流 × 时间。假设电池的电压不变，我们就可将 mA · h作为常规单位。电池容量值除以消耗的平均电流即为电池的预期寿命。这样，我们所需要做的就是计算设备消耗的平均电流。

电池通常是突然枯竭的，而不是平稳枯竭的：现代的电池擅长于保持电压，结果导致能耗不能平稳的下降。电压为 $U$、电阻为 $R$ 时，使用功率 $U^2/R$ 是一个常数。一旦电池能量耗尽，电池就会突然失效。某些防护设备将可以通过测量已使用的能量，来计算出电池的剩余寿命。为了实现此任务，防护设备需要测量电池输出的电流。于是，电池的剩余寿命将为电池满能量时的容量（mA · h）减去已使用的能量（mA · h）。

WirelessHART 现场设备主要有三种电流消耗源：处理器、射频部分和工业设备。在本小节中，我使用一个简化的案例来描述计算过程。在该案例中，假设设备每隔 15 s 发布一次数据。

（1）处理器　我们利用飞思卡尔公司的 MC1322™芯片作为参考。该处理器在正常操作时的电流消耗为 3.3mA。MC1322™ 有两种睡眠模式：“hibernate” 和 “doze” 模式。这两种模式除了时钟精度外彼此非常相似。“doze” 模式使用的是外部时钟并消耗更多的电流，但是设备在苏醒后有更好的机会保持时间同步。因此，我们不得不选择 “doze” 模式。MC1322™处理器在 “doze” 休眠模式时电流消耗为 60μA，而在活跃模式时电流消耗为 3.3mA。假设在 15 s 的发布时隙内仅有一次

活动状态，那么该处理器的平均消耗电流为62μA/s。

（2）射频部分　MC1322™是系统集成芯片，其射频部分是内置的。MC1322™的射频部分在接收信号时的电流消耗为24mA，在发射信号时的电流消耗为29mA。假设没有外部射频部分，当发送一个43字节长的数据报文（1568 μs）和接收一个确认包（1124μs）时，MC1322™射频部分的平均电流消耗为4830μA/ s。

（3）工业设备　传感器设备在测量时也会消耗电流。我们采用温度传感器来举例说明。通常，温度传感器的每次测量需要花费120 ms和消耗500μA。因此，温度传感器的平均电流消耗为4μA/s。

（4）电池　我们使用两个5号电池。单个电池的容量是2000mA·h。

（5）合计　为了简便起见，我们不考虑状态变化期间所需要的能耗。这样，两个5号电池将能持续816 h，稍微多于一个月。然而，过程工业车间通常要求电池的使用寿命超过一年。因此，在该案例中，两个5号电池是不够的。最后，值得注意的是电池本身提供的能量是变化的。在非常规工作温度时，耐酸铅型电池的使用寿命可能会减半。其他不突出的因素也可能影响电池的使用寿命，例如释放频率和持续时间、电压变化、连接、自放电的泄露等。

## 9.9　互操作性和互换性

不同供应商的不同设备工作在一起对于标准来说是很重要的，这包括互操作性和互换性。互操作性是指一个设备能与另外一个设备通信；互换性是指在不改变网络行为的情况下，一个设备能取代另外一个设备。

互操作性对于标准来说是必不可少的。但是，互换性在某些标准中并未被要求。互操作性和互换性功能在WirelessHART标准中都是强制要求的。在WirelessHART标准中，互操作性的概念涵盖了互操作性和互换性功能，其定义为“互操作性是一种能力。这种能力能使不同制造商的设备工作于同一系统，并使设备的替换不会导致上位机系统层的功能丧失”。

设备还可能拥有定制功能，甚至也可能被用于定制的应用。这些定制的功能不应该妨碍或取代WirelessHART标准中定义的功能，也不应该期望WirelessHART网络能保证定制应用的性能。

## 9.10　WirelessHART网络的非期望访问

在本小节开始之前，需要强调的是WirelessHART标准有着非常强的可靠性和安全性。我们接下来讨论的内容并不是使WirelessHART变得可敬，而是在一定程度上揭示任何无线网络都面临的普遍危险。

### 9.10.1　拥塞

WirelessHART 网络能处理无意识的短暂拥塞，并且处理得非常好。目前，绝大部分无线网络都不能很好地处理有意识的拥塞，WirelessHART 网络同样也不能很好地处理有意识的拥塞。

WirelessHART 标准采用 IEEE 802.15.4 标准，并使用 2.4GHz 频段作为其物理信道。拥塞 WirelessHART 网络的一个直接办法是在所有的 16 个信道中持续不断地发送噪声信号。当然，我们这里将研究智能化的拥塞，即仅在特定的时间点产生拥塞以使 WirelessHART 网络无效。

由于 WirelessHART 数据链路层的载荷没有被加密，而其网络层的载荷被加密，所以任何抓包器都可以轻易地解析出网络层头部之前的报文内容。当然，伪造报文仍然需要网络密钥，因为伪造报文的消息完整性代码（MIC）依赖于该网络密钥。虽然入侵者能够获得报文，但是他无法知道报文的应用层内容，因为应用层内容在网络层被加密了。

WirelessHART 网络是全网同步的，所以入侵者仅需在一个非常短的时间内拥塞信道就能扰乱整个网络。就像任何入网设备一样，入侵者可以先侦听并与网络同步。与任何 WirelessHART 网络的同步不需要安全信息。于是，拥塞就变得非常有效。对于 CCA 使能的网络，我们仅需要在设备执行 CCA 的时候制造出噪声信号。对于 CCA 不使能的网络，我们仅需要拥塞报文的前同步信号。假设我们有低成本、长电池使用寿命（和智能）的入侵者。那么我们仅需要 16 个这样的入侵者便能瘫痪整个 WirelessHART 网络。传统的干扰机通常要一直不停地工作，并且价格昂贵。

使网络崩溃的攻击不需要持续太长的时间。仅少许时隙（例如长于最大重传时间）就足够中断一条链路，甚至能使设备退出网络。

正如任何入网设备一样，敌对者也可能跟随跳信道序列持续拥塞某个链路。最容易跟随的跳信道序列是加入链路的跳信道序列，因为该序列可以非常容易地从广播报文中获知。入侵者能阻碍任何设备入网。

入侵者也能够推知任何链路的跳信道序列。任何链路的活跃信道可以通过已知公式计算出。让一个 16 信道的抓包器持续运行一段时间，我们就能识别出活跃信道数。进一步地，如果已知活跃信道和 ASN，我们就能推断出链路的信道偏移量。接着，超帧大小也能从两个设备间的传输模板猜测出。有时候，广播报文中列出了超帧。这时，超帧大小就显示在报文的文本信息中。给定超帧大小，超帧内的链路时隙数也就可以被猜测出来了。

拥塞有可能很严重从而造成 WirelessHART 在某些应用的“停止演出”。幸运地，当 WirelessHART 网络中的某部分无反应时，WirelessHART 标准中的某些方法能告知所有节点该部分正在发生拥塞。例如，网络管理器能利用信道黑名单、邻居

健康报告和“path-down”警报。由于 IEEE 802.15.4 射频的相对低功耗和短距离，拥塞设备将不得不被放置在工厂内或者使用非常高的发射功率。这两种情况都有可能引起工厂车间员工的警觉。

## 9.10.2 密钥的发现

数据链路层有两种密钥——公共密钥和网络密钥。公共密钥是公开的，而网络密钥被所有网络设备所共享。每个会话的网络层密钥是唯一的，但是简单的报文头部揭示了正在使用的是哪个会话。除非通过网络外获得密钥，那么入侵者发现密钥的唯一途径就是采用逆向工程。在每个采样数据，随机数（nonce）能从未被加密的文本部分中构建。MIC 和密文是已知的。那么，剩下的任务就是从采样序列中猜测出密钥。如果猜测出的密钥能针对密文产生同样的 MIC，那么该密钥就是正确的。

WirelessHART 和 IEEE 802.15.4 标准都使用 128 位的 AES 密钥。理论上讲，密钥发现需要巨大的采样序列和很长的采样时间。此外，WirelessHART 标准要求周期性地更换密钥。这样，由于入侵者不知道新密钥何时被使用，所以采样序列中可能包含了不同密钥加密后的报文。因此，密钥的更换也就破坏了入侵者的采样序列，从而使得密钥更不可能被轻易窃取。

# 第 10 章　一 般 话 题

摘要：在这一章中，我们将讨论一些与 WirelessHART 标准相关的一般话题。这些话题包括有：WirelessHART 标准与 OSI 网络层次模型的关系、射频基本原理、集中控制、现场勘查、WirelessHART 标准与 IEEE 802.15.4 标准的关系、共存、其他现场总线、WirelessHART 系统的局限性、安全和可靠性以及 WirelessHART 对用户意味着什么。这些话题被罗列成小节标题。

## 10.1　WirelessHART 标准和 ISO OSI 标准

所有网络通信协议基本上都参照了国际标准化组织（International Organization for Standardization，ISO）提出的开放式通信系统互连参考模型（Open System Interconnection Reference Model，OSI）。OSI 模型将网络功能分成 7 层。OSI 模型是非常完整的。所有的网络功能都能在该模型中找到对应的位置。该重要模型能有助于通信协议栈的规划和设计。

OSI 协议模型覆盖全面，且各层功能彼此独立。这样，协议栈具体实现时可以把某些层结合在一起，也会把 MAC 层从数据链路层中分离出来的。嵌入式系统编程往往不得不在优雅和性能之间权衡。像其他嵌入式系统一样，WirelessHART 标准并没有包含 OSI 模型中所有 7 个协议层。WirelessHART 标准旨在简化、消除或跨层优化 OSI 模型中定义的功能。第 1 章中的图 1-4 描绘了 WirelessHART 协议栈与 OSI 模型的对比。以下一些因素导致了 WirelessHART 标准与 OSI 模型的差异。

（1）电源　电源消耗是嵌入式系统需要考虑的一个主要问题。WirelessHART 现场设备通常是电池供电的，因此支持完整的 7 层协议栈不是最好的解决方案。

（2）速度和尺寸　嵌入式系统的处理器和存储器尺寸通常是较小的。因此，实现一个完整的 OSI 7 层协议栈不是一个理想的解决方案。

（3）安全　OSI 模型开始于 20 世纪 70 年代。当时，安全被认为是一个重要因素，但不是最重要的因素。现今，安全变成了网络中最重要的因素。因此，许多非常复杂的安全技术已经被开发出来。WirelessHART 在数据链路层和网络层都采用了 128 位加密算法和 CCM* 认证算法。

（4）实时性　嵌入式系统中的另一个重要要求是网络数据的有保障递送。基于此，WirelessHART 标准采用 TDMA 机制和全网同步。WirelessHART 网络中所有的协议栈都定义了时间参数。

因此，大部分工业网络协议都是 OSI 模型的子集。

（1）上层 协议栈的底层对于网络设计和实现是必不可少的，为了达到简化协议栈的目的，所以现场总线通常简化或完全去除协议栈的一些上层。除了减少协议实现所占用的空间和节省功耗，大多数嵌入式协议栈都不需要 OSI 模型中定义的一些特色。WirelessHART 标准去掉了表示层，将表示层的部分功能融入了应用层。同时，WirelessHART 标准将会话层合并到网络层，并保留了一个简单的传输层。

（2）跨层优化 WirelessHART 标准除去了传输层中对数据分割和重组的支持。WirelessHART 应用层采用块数据传输（block data transfer）模式来处理大块数据。WirelessHART 网络层负责管理会话。

另一个优化对象是图路由。在 OSI 协议模型中，路由功能位于网络层。然而，在 WirelessHART 协议模型中，数据链路层也参与了图路由。对于图路由，如果某个设备有多个可转发的目标设备，那么与其让网络层选择哪个目标设备来转发报文，到不如让网络层发送图 ID 给数据链路层，再由数据链路层来决定。在 WirelessHART 标准中，数据链路层保存了图路径的转发设备列表。数据链路层选取第一个链路来给转发设备列表中的设备发送数据。这种方法的好处是如果传输失败了，数据链路层能在不需要网络层参与的情况下尝试重传报文给所有转发设备直到超时。否则，设备的数据链路层仅向一个邻居设备重传报文，而设备的网络层用来向替代的邻居设备重传报文。同时，在 WirelessHART 标准中，链路是在数据链路层配置的，网络层可能不知道那个设备有最早的可用链路。此外，数据链路层和网络层之间的报文传递存在着延迟，因此让网络层来决定向哪个邻居设备转发报文是效率低的。即使网络层已经选择了最早的可用链路，但是当报文到达数据链路层的时候，网络层选取的链路可能已经不可用了。

## 10.2 射频基本原理

### 10.2.1 射频基本原理

#### 10.2.1.1 电磁波

微波、FM/AM 无线电波、电视信号、手机信号、光等都是连续的电磁波，与池塘中的水波相似。包括光在内的所有电磁波都以同样的速度传播——光速传播。同时，电磁波的传播速度又等于频率和波长的乘积。这些电磁波都可以用正弦曲线来表征，但是各自的震动频率不同。因此，我们也可以说所有的电磁波只是频率不同。量子力学的物理学家使我们明白电磁波也是离散的量子。但是幸运的是在无线网状网络世界里我们不需要理解电磁波的量子特性。

#### 10.2.1.2 发送与接收

电磁波在电场与磁场之间连续地切换。天线中的电流周期性变化即可产生出电磁波。射频变频器是一种特殊的电子电路，其能控制向天线充电或放电来产生不同的电磁波。于是，处理器能通过控制变频器来发送期望的电磁波。天线也能被电磁波触发来产生变化的电流，变频器能检测到这种变化的电流。因此，处理器也能接收到来自于电磁波的信息。如果我们能将数据隐含在电磁波中，那么我们就能实现一个处理器向另外一个处理器无线地发送报文。这也正是现代无线通信的基本原理。

无线信号的发射能量可以被用来表征发送方的特性。无线信号的发射能量被定义为有效辐射功率（Effective Radiated Power，ERP），其单位为分贝（dB）。ERP依赖于整个射频电路，多少能量被利用了，多少能量被射频电路以热量形式损失了等。ERP还取决于天线是如何布置的。具有相同ERP的两个天线将显出相同的传输能力。通常，天线是全方位的，即其向四面八方辐射。其中，发射功率最强的方向被用来测量天线的增益。天线增益是在输入功率相等的条件下，实际天线与理想的辐射单元在空间同一点处所产生的信号的功率密度之比。全向天线的传送功率在各个方向均等。等效全向辐射功率（Equivalent Isotropically Radiated Power，EIRP）是无线电发射机供给天线的功率与给定方向上的天线绝对增益的乘积。

接收方的特性可以用接收信号能力来表示，即接收灵敏度。其有两个衡量标准：信噪比（SNR）和接收信号强度指示（RSSI）。信噪比是接收信号功率与白噪声功率的比值。一个好的接收器能够在低信噪比环境中提取出信号信息。有时信号的干扰不完全是白噪声，而是同一信道上的其他合法传输信号。这时可以用信号与干扰和噪声比（Signal to Interference-plus-Noise Ratio，SINR）来衡量。RSSI则用来描述接收到的信号的功率强度。一个好的接收器能够识别出RSSI值低的信号信息。

天线的大小和形状决定了最佳频率和天线增益分布。WirelessHART设备使用的常用天线是一个约10cm长的单天线。天线有时候被绘制在印制电路板上，即PCB天线。PCB天线是一种内置天线，它可以减少系统的物理尺寸但是传输距离相对较短。

#### 10.2.1.3 传输空间

现在让我们看看在发送者与接收者之间的传输空间。无线信号的最佳传输路径是发送方与接收方之间没有障碍物的直接路径，如发送方到接收方的直视路径（line-of-sight，LOS）。接收方通过直视路径能得到最好的接收效果。在许多情况下，位于直视路径上或靠近直视路径的障碍物都会引起信号的反射和丢失。术语“非直视路径（Non-line-of-sight，NLOS）”用来描述这类障碍物的存在。发送方和接收方之间的区域被分为菲涅耳区（Fresnel Zone），以科学家菲涅耳命名。如图

10-1 所示，所有菲涅耳区一起构成的形状像一个扁长的椭球体。每个菲涅耳区是一个椭圆旋转层。发送者和接收者位于回转椭圆体的两端。放置在不同菲涅耳区里的障碍物将导致不同的干扰模式。两个收发器之间的直接线路是第一个菲涅耳区。如果该区畅通，那么该区将会提供最强的信号。传输空间又可分为室内和室外。非直视路径（NLOS）通常存在于室内，而直视路径（LOS）大多数情况下发生在室外。

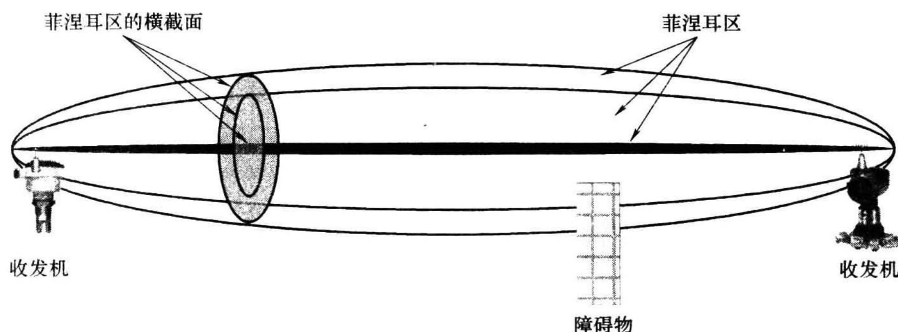



图 10-1　菲涅耳区

在过程工业车间里，许多工业设备通常使得长直视路径不可能存在。信号路径经常被反射，这样接收方就会接收到多个到达时间不同的相同信号，这也被称为多径传播。多径传播是非常普遍的。由于多径信号的相互抵消，多径传播可能会降低信号的接收质量。对某信号的最强干扰常常是其反射信号。

过程工业车间里的设备不仅阻碍了直视路径（NLOS），而且通常还会吸收信号。这必然会削弱信号，这就是所谓的路径衰落。引起路径衰落的原因有很多，也有很多路径衰落模型来研究它们。自然衰落是传输距离引起的。通常情况下，信号强度四倍反比于信号的传输距离。

另一种常见的干扰来自于其他周边设备的通信，即所谓的“远—近问题”。假设设备有一个近邻设备和一个远邻设备，该设备需要从远邻设备接收报文。如果近邻设备碰巧同时也发送报文，由于信号衰减，近邻设备发出的信号强度比远邻设备发出的信号强度要大得多。即使近邻设备发出的信号可被认为是噪声，但是该噪声可能由于太大而无法被滤除掉。

#### 10.2.1.4　编码和调制

我们已经讨论了电磁波。但是，我们想要做的是将信息从发送方传递到接收方。利用普通正弦波的不同调制方式可以将数据转换成电磁波。接收方检测到这些被使用的电磁波并从中解析出数据。这就是所谓的调制和解调。被使用的某些频率的电磁波称为载波。例如，AM 调制无线电信号的幅度；FM 调制无线电信号的频

率。我们还可以调节信号的相位、方向或这些的组合。AM/FM 无线电是模拟的。数字数据需要经历另外一个步骤，即编码和解码。原始数字数据被表示成 0 和 1 的序列。编码器将这些 0 和 1 序列编排成某些数值，并将这些数值提供给调制器。在接收方，解调器输出这些数值，然后解码器将这些数值解析成对应的 0 和 1 序列。

### 10.2.2 扩频调制

据预计，在发送方发送一些数字数据到接收方的整个过程中，许多因素都可能引入错误。成功的调制方法之一是扩频。扩频技术为一个通信任务而同时占用多个频段。两个典型的扩频技术是直接序列扩频（direct sequence spread spectrum，DSSS）和跳频扩频（frequency hopping spread spectrum，FHSS）。

物理信道是指围绕某一频率的一段频宽，它是通信介质的一个单元。不同的信道能同时被不同的通信使用。扩频通信技术为一个通信而占用多个信道。如果其中某个信道不可用了，其他的信道仍能让信号通过。

#### 10.2.2.1 直接序列扩频

直接序列扩频（DSSS）系统同时使用多个信道。信号发射功率被分摊到这些信道。每个信道上传送的实际数据是对原始数据用伪噪声码编码后的数据。接收方使用同样的伪噪声码合并多个信道的数据，并还原出原始数据。一个信道上的干扰只会影响整个数据的一部分。使用一些错误恢复编码，接收方就能对此类干扰有免疫力。因为发送方使用直接序列扩频技术能将能量均匀分布到多个信道，所以其传输的信号对于其他设备而言更像白噪声。

直接序列扩频（DSSS）有助于解决“远—近问题”。虽然近邻设备发出的信号仍然以噪声的形式存在，但是远邻设备发出的信号会以被成倍增强，增强的倍数为信号所占用的信道数。因此，信噪比（SNR）通过乘以信道数而被增强了。

#### 10.2.2.2 跳频扩频

跳频扩频（FHSS）并不将其发射功率扩展到多个信道。相反，它会在某个时刻从多个信道中伪随机地挑选出一个信道来发送信号。例如，8 个不同的物理信道可能被用来发送一个字节的 8 位数据。接收方按同样的方式跳信道以保持同步通信。同样，由于内置了额外的纠错字节，在某个信道上的信号丢失将不会破坏整个数据报的传输。

跳频扩频（FHSS）也有助于解决“远—近问题”。由于近邻设备与远邻设备使用不同的跳信道序列，在大多数情况下，它们会占用不同的信道来通信。在极少数情况下，近邻设备与远邻设备占用同一通信信道从而干扰远邻设备，那么远邻设备只需简单地放弃此次通信并在其他可用信道上再次通信。

#### 10.2.2.3 WirelessHART 标准使用了什么

WirelessHART 标准在不同层面采用了 DSSS 和 FHSS。DSSS 被用于每个 Wire-

lessHART 报文的传输，而 FHSS 被用于确定每次 WirelessHART 时隙通信所选用的信道。

WirelessHART 标准采用了 IEEE 802.15.4 标准的 2.4GHz 频段的物理层。该物理层使用了 16 个状态的准正交调制技术，并采用偏移四相移相键控（O-QPSK）方式将最后的编码序列调制到无线电信号。IEEE 802.15.4 标准在 2.4GHz 频段定义了 16 个毗连的信道。O-QPSK 调制方式没有扩展到所有 16 个信道，所以不能称为直接序列扩频。但是，它像直接序列扩频一样将每个信道分为多个子信道，然后将信号扩展分布在这些子信道上。

WirelessHART 标准在更高层面上使用了跳频技术。该跳频技术的信道跳跃方式不是基于每个比特位的，而是基于每个报文的，更准确地说是基于每个时隙的。

### 10.2.3 介质访问控制

介质访问控制子层是数据链路层内的底层。数据链路层控制着对物理层的访问。介质访问控制子层控制着何时以及如何发送和接收报文。

#### 10.2.3.1 单工和双工

网络节点既能发送也能接收数据。对于许多有线网络，一个节点可以同时发送和接收数据，这样的节点是双工的。如果一个节点只可以发送或接收，但不能同时发送和接收，那么该节点是单工的。WirelessHART 网络中所有的无线设备都是单工的设备。

#### 10.2.3.2 CSMA and CSMA-CA

CSMA 是载波监听多路访问（Carrier Sense Multiple Access）的缩写，而 CSMA-CA 是带有冲突避免的载波侦听多路访问（CSMA with Collision Avoidance）的缩写。在 CSMA 机制中，已准备发送数据的设备首先侦听信道。如果该信道是空闲的，那么该设备就开始发送数据，否则该设备将等待直到信道空闲。CSMA 中的 MA（Multiple Access，MA）意味着多个设备可能要在同一信道同时发送数据。在 CSMA-CA 机制中，设备不是持续等待直到信道空闲，而是等待一个随机的时间。这能防止所有试图发送数据的多个设备之间的不断冲突。

CSMA 或 CSMA-CA 解决不了所谓的隐藏节点问题。如果设备 A 能与两个设备通信，而这两个设备彼此之间不能相互通信，那么这两个设备在某一时刻可能都会认为信道是空闲的，从而同时向设备 A 发送数据。这样，这两次数据传输在设备 A 处就会相互干扰，从而将导致这两次数据传输的失败。这两个设备中的任一设备对于另一设备来说就是一个隐藏节点。

#### 10.2.3.3 TDMA

TDMA 是时分多址（Time Division Multiple Access）的缩写。通信信道被分成

了许多个时隙，设备使用分配给自己的时隙来发送数据。因为多个设备会被调度成不会同时发送数据，所以 TDMA 机制能避免冲突的发生，也能解决隐藏节点的问题。这里的多址（Multiple Access，MA）意味着同一信道能被多个设备在不同时间多次访问。

#### 10.2.3.4 自动重传请求

ARQ 是自动重传请求（Automatic Repeat Request）的缩写。ARQ 机制要求确认报文的接收。双向握手保证了报文的接收。如果发送方没有收到确认报文，那么发送方将重传或者在重传多次后报告失败。对于 ARQ 机制，一种罕见的情况可能发生，即确认报文已经发送但没有被接收到。这时，发送方会认为报文传输失败了，但接收方却认为报文传输成功了并且自己对该报文做出了确认。

#### 10.2.3.5 WirelessHART 标准使用了什么

IEEE 802.15.4 标准采用了 CSMA-CA 机制。虽然 WirelessHART 标准采用了 IEEE 802.15.4 标准，但是 WirelessHART 标准只采用了 TDMA、ARQ 以及 CSMA-CA 的部分概念。在过程控制领域，保证过程数据的可靠传输是必不可少的。TDMA 满足了这种要求。WirelessHART 标准中的每个时隙都是 10ms。在一个时隙内，每个信道通常只有一个设备被配置为发送报文，并在同一时隙内接收确认报文。

CSMA 机制对于非实时数据也是有其自身的优势的，尤其是当非实时数据的发送频率较低时。WirelessHART 网络为 CSMA-CA 分配多个接入时隙。这些时隙被称为共享链路。在共享链路中，多个设备可能发送数据，一个设备侦听数据。因为所有的设备都是同步的，所以多个设备可能同时检查信道并发现该信道是空闲的。这时，这些设备就都可能会同时发送数据，并且都不知道其他设备的存在，从而导致冲突的发生。这种冲突可以通过是否没有接收到确认报文来后验检测到。如果发生这种情况，所有发送方将退避一个随机时隙数后再发送数据。

### 10.2.4 使用 2.4GHz 频段的原因

WirelessHART 网络使用的是 2.4GHz 频段，这是从 IEEE 802.15.4 标准继承而来的。使用该频段，1km 范围内的下雨或下雪的影响是可以忽略的。2.4GHz 是 ISM（工业、科学和医疗）频段之一，是在全世界范围内都无需授权的无线频段。换句话说，该频段的使用是免费的。授权频段的另一个缺点是同一频段在不同国家用途可能也不同。像 WirelessHART 技术这样的国际标准必须在国际上尽可能地被广泛使用。符合标准的设备在一个国家可以使用但在另一个国家不能使用，这对 WirelessHART 标准而言是不能接受的。

当然，WirelessHART 网络使用 2.4GHz 频段的缺点是它必须与其他网络竞争使用该频段。好消息是，先进技术在这个领域内的发展使得多种不同网络间的共存变得更容易，我们将在本章的后续部分讨论此问题。

## 10.3 集中控制

在集中控制模式中，节点不产生自己的调度，而是执行由中央调度器（如基站）产生和下载的调度。节点只需简单地收集通信统计资料，并发送给中央调度器。在分布式控制模式中，节点是自组织的，它调度自己的任务和数据处理，也处理来自于邻居节点和上位机的请求。在集中式网络中，中央控制器产生路由路径并分发给每个节点。在分布式网络中，每个节点通过与其他节点的交流来建立自己的路由信息。

集中控制有利于过程工业的实时性（Song 等人，2007 年）。WirelessHART 标准定义了一个唯一负责管理整个 WirelessHART 网络的网络管理器。自组织无线网络中的节点通常到处徘徊、随机加入和离开网络，而工业车间里的无线节点通常是位置固定的，它们被放置在应该感应或执行的地方。因此，WirelessHART 网络中的数据路由也是可以预先确定的，这使得集中配置和保证数据传递成为可能。以下几点促成了 WirelessHART 网络采用集中控制模式。

（1）运行调度　在集中控制模式中，设备将接收网络管理器发出的、准确的数据路由调度信息。固定时隙将被分配用来路由应用数据。网络管理器也将调度网络设备使得它们能为其他设备路由数据以及发送自己的数据。当不执行以上调度任务的时候，设备可自由处理自己的内部任务。在集中控制模式中，设备将不会在调度上成为造成错过任何最后期限的原因。

如果设备的调度是由设备自己决定，而不是由网络管理器统一调度的，那么设备将遵照自己的判断来处理应用数据。该设备也可能不会为转发其他应用数据分配更高的优先级。这样，数据传输的延迟将无法预先确定。此外，即使该设备有专门用于数据路由的时隙，它也无法区分来自不同应用的数据。这意味着，应用程序共享路径将引起在路径方面的相互干扰，这对满足实时要求带来了更多的障碍。

（2）数据路径的产生　集中管理在产生路由路径方面有优势。考虑到所有可能存在的链路，并基于负荷、跳数、信号强度及更重要的时限要求，网络管理器能为每个节点推导出最好的路由表。节点所需要做的是发现自己的邻居节点、测量与其邻居节点的信号强度，并将这些信息发送给网络管理器。

如果每个节点对网络都各自形成各自的认识，那么数据路由将会变得非常困难。一个好的路径可能被所有的数据传输占用，那么这条受欢迎的路径上的节点将会比其他节点先耗尽电池。人们总是可以找到好的分布式路由协议，但无论这些协议是什么，它们总是可以在中央控制器里实现。

（3）设备加入和离开　我们现在分析一个节点如何处理与其邻居节点的往来。

假设网络在某个新设备加入网络之前正在运行任何没有违反实时性的应用程序，该新设备在加入网络后要求与网络中的某些节点进行数据通信。如果这些新增的数据流量没有被正确管理，那么新设备可能会干扰其他应用数据并导致它们通信失败。此时，新设备的邻居设备应该给该新设备的数据分配最低的优先级，但是在分布式控制中，新设备的邻居设备可能给新设备的数据分配了与现有应用程序一样的优先级。另一方面，各个节点独自作出这样的决定是非常困难的。

对于集中式控制，新入网的设备在没有得到网络管理器许可之前甚至可能不能发送数据。在网络管理器认为新节点的加入将不会影响现有系统之后，新设备才能安全地被允许加入网络并发送数据。

当一个设备死亡或自愿离开网络时，采用分布式控制方式更好。如果该设备是网络末端节点，那么集中式和分布式这两种控制方式之间没有太大的区别。如果该设备是路由节点，那么其邻居设备的数据必须被重新路由。集中式控制将不能很好地响应这种重新路由的要求，因为新的调度必须由中央控制器来更新。然而，在分布式控制中，设备可以本地自行处理重新路由。

（4）冲突避免　集中调度的另一个优点是可以避免冲突。在随机信道接入机制（如 CSMA）中，需要发送数据的节点首先侦听信道，如果该信道是空闲的，那么该节点就开始发送数据。如果该信道被占用，那么节点不得不退避一段时间后再试。这种机制当网络流量比较低的时候工作得非常好。然而，一旦许多节点在同一时间都要发送数据，许多冲突就会发生并导致错过最后时限。而在集中调度模式中，一个时隙是专门用于一次传输，重传仅用于处理外界的干扰，这一点在下一小节中阐述。

（5）临时干扰　临时干扰在无线网络中是很常见的。很多方法都可以用来缓解这一问题，如 DSSS 和 FHSS。然而，这些方法都无法完全消除临时干扰的问题。我们不得不在调度策略范围内考虑此问题以满足实时性的要求。当计算最大数据传输延迟时，我们应该考虑到重传和重新路由。对于临时干扰，集中式和分布式控制对重传和重新路由的要求相似。对于这两种控制模式，发送方都将向同一邻居重新发送数据报；如果不成功，则尝试向替代路径上的邻居重新发送数据报。分布式控制可能有的优势是节点能根据失败信息重传或重新路由。例如，它可以选择之前传输最成功的节点作为替代邻居。而在集中控制模式中，节点可能在同一失败的路径上一直重传直到中央管理器告知其使用其他的路径。

（6）负担分配　通常，集中式控制减少了独立节点的调度计算，这样反过来又降低了传感器的成本、延长了节点的电池使用寿命。实时和非实时的应用都可以在这方面受益。

## 10.4 现场勘查

现场勘查有助于无线网络的部署。现场勘查主要包括两个部分：一个部分是在目标现场测量已有无线系统的布置情况；另一个部分是在规划的网络拓扑结构下测量信号传输的路径衰落特性。一个典型的过程工厂车间是一个管道和设备构成的迷宫。这些管道和设备大部分都会反射和吸收无线信号。过程工业车间的现场勘查结果通常高度依赖于实际现场情况，并有助于无线网络在过程工业车间里的设计和部署。

现场勘查也有其自身的问题。首先，现场勘查工作通常是不容易的。然而，无线网络的布置应该比有线网络更简便。其次，设备在工厂车间里的位置并不是完全固定的。虽然大多数过程设备的位置都是不变的，但是其他一些可移动的设备（如材料、产品和车辆等）都可以很容易地改变频谱分析仪捕获到的现场模式。因此，现场布置之前现场勘查一次是不够的。每当工厂车间内发生了变化，我们是否都需要再次现场勘查？第三，无线设备不能被随意地部署在工业现场。它们的位置更可能是作为现场部署规划的输入，而不是作为现场部署规划的输出。如果将无线设备的位置作为现场部署规划的输入，这也就削弱了现场勘查的实际价值；现场勘查应该是帮助确定无线设备的最佳部署位置。

WirelessHART标准没有强制规定现场勘查。设备部署位置不受信号强度和干扰的约束。WirelessHART标准使用固有的网状网络技术来实现可靠的通信。如果某条非冗余路径在某些时候变得很脆弱，那么对应的解决办法是在这些薄弱的地方增加额外的路由器设备或接入点，并让网络管理器将该非冗余路径清除掉。此外，这些额外的设备可以被放置在任何便于布置的地方。

## 10.5 WirelessHART标准和IEEE 802.15.4标准

本书一直重复提到WirelessHART标准采用了IEEE 802.15.4标准。任何WirelessHART报文都是一个合法的IEEE 802.15.4-2003未加密的数据报文。IEEE 802.15.4-2006标准是IEEE 802.15.4的最新版本。在本节中，我们更详细地总结了在最新版本中什么被丢弃了、什么仍然保留了、什么被改变了。

### 10.5.1 IEEE 802.15.4头字段中WirelessHART值

WirelessHART报文的物理层头部与IEEE 802.15.4报文的物理层头部完全相同。接下来，我们关注MAC层头部（见表10-1）。

表 10-1 IEEE 802.15.4 帧控制字段

| IEEE 802.15.4 名称 | 比特位 | WirelessHART 值 | 解释 |
|---|---|---|---|
| 帧类型 | $b_2b_1b_0$ | 001 | 类型为数据 |
| 安全使能 | $b_3$ | 0 | 没有 IEEE 802.15.4 定义的安全 |
| 帧挂起 | $b_4$ | 0 | 没有帧挂起 |
| 要求确认 | $b_5$ | 0 | 没有 IEEE 802.15.4 的确认 |
| PAN 内部 | $b_6$ | 1 | PAN 以内 |
| 保留 | $b_9b_8b_7$ | 000 | — |
| 目标地址模式 | $b_{11}b_{10}$ | 10 或 11 | 短地址或长地址 |
| 保留 | $b_{13}b_{12}$ | 00 | 在 IEEE 802.15.4-2006 中被定义为帧版本，意味着与 IEEE 802.15.4-2003 相兼容 |
| 源地址模式 | $b_{15}b_{14}$ | 10 或 11 | 短地址或长地址 |

## 10.5.2 安全方式

在 IEEE 802.15.4 标准的 MAC 层中，一个安全选项是使用 CCM* 加密机制。WirelessHART 标准也采用了 CCM* 加密机制，但是与 IEEE 802.15.4 标准的使用方式有所不同。WirelessHART 标准采用了 IEEE 802.15.4 标准的无加密版本，并将安全信息 MIC 放置在 IEEE 802.15.4 MAC 层有效载荷中，请参阅表 10-2。WirelessHART 标准不加密数据链路层的有效载荷，使用 CCM* 生成 MIC 来实现认证。数据链路层的有效载荷是网络层数据。由于网络层仅加密自己的有效载荷，所以数据链路层头部和网络层头部都没有被加密，这样任何能捕获 WirelessHART 报文的设备都可以轻易地获得数据链路层头部和网络层头部中的信息。IEEE 802.15.4 标准并没有定义网络层。在 WirelessHART 网络中，路由信息不需要被加密。因为网络层的有效载荷被加密了，所以不加密路由信息也不是一个很大的安全风险。网络层的加密方式不出人意料的也是 CCM* 加密机制。用于认证的 MIC 也被包含在网络层头部中。

目前商业化的 IEEE 802.15.4 芯片通常都含有 CCM* 算法硬件加速器。为了使 WirelessHART 设备能充分利用这一优势，这类芯片应该向软件实现直接公开其 CCM* 应用程序编程接口（API）。如果 CCM* 算法硬件加速器被另外嵌入在 IEEE 802.15.4 MAC 安全处理器中，那么我们就不那么幸运了而不得不自己编写软件来实现 CCM* 算法。

表10-2 IEEE 802.15.4 MAC层头部

| IEEE 802.15.4名称 | 字节 | WirelessHART值 | 解释 |
|---|---|---|---|
| 帧控制字节1 | 低字节 | 0x41 | 参见表10-1 |
| 帧控制字节2 | 高字节 | 0x88，0x8C，0xC8 | 参见表10-1。没有可能出现0xCC的情况 |
| 序列号 | 1 | ASN的最低有效字节 | 与IEEE 802.15.4的定义不同 |
| 目标PAN标识符 | 0/2 | 2字节 | 网络标识符 |
| 目标地址 | 0/2/8 | 2或8字节 | 短地址或长地址 |
| 源PAN标识符 | 0/2 | 0字节 | 默认 |
| 源地址 | 0/2/8 | 2或8字节 | 短地址或长地址 |
| 帧载荷部分1 | 1 | — | DLPDU分类符 |
| 帧载荷部分2 | 0..111 | — | DLL载荷 |
| 帧载荷部分3 | 4 | — | MIC |
| FCS | 2 | FCS | CRC代码 |

### 10.5.3 MAC层的最大有效载荷

IEEE 802.15.4报文的最大长度是133个字节。物理层头部占用了6个字节。因此，MAC层最大长度为133-6=127个字节。MAC层头部和尾部的最小长度是9个字节。没有安全字段的MAC层头部的最大长度为25个字节。因此，MAC层的最大有效载荷根据MAC头部格式而处于127-25=102个字节与127-9=118个字节之间。然而，IEEE 802.15.4-2003标准为了安全起见而选取较小的102个字节作为其MAC层的最大有效载荷数。后来，IEEE 802.15.4-2006标准放宽这一限制。如果某报文中的版本字段表明其是2006版本的，那么该报文的MAC层有效载荷可能多于102个字节。请参阅IEEE 802.15.4-2006标准中的表85。

一个WirelessHART报文也是一个IEEE 802.15.4-2003报文。WirelessHART的数据链路层头部对应着IEEE 802.15.4 MAC层的头部。WirelessHART数据链路层头部的长度为11个字节，或者在设备地址为长地址的情况下为17个字节。IEEE 802.15.4 MAC层有效载荷中的5个字节用于存放WirelessHART数据链路层的额外字段。WirelessHART标准仍然允许最大报文长度为133字节，这意味着它的数据链路层最大有效载荷为127-11-5=111个字节或127-17-5=105个字节。因此，对于WirelessHART报文中对应着IEEE 802.15.4 MAC层有效载荷的部分，如果其长度超过了102个字节，那么该报文就不再会被认为是IEEE 802.15.4-2003报文。然而，如果IEEE 802.15.4-2006接收器收到这样的报文后，接收器会自动更正其帧中的版本字段。

### 10.5.4 其他方面的比较

1）IEEE 802.15.4 标准的预计应用领域是个人区域网络（Personal Area Network，PAN）。个人区域网络的覆盖范围通常为 10m 左右。然而，WirelessHART 标准定位于覆盖范围更大的过程工业领域。

2）IEEE 802.15.4 设备的发射功率预计比较低，通常为 0dBm。WirelessHART 标准规定设备的发射功率为 10dBm，这也是 2.4GHz 频段在许多国家被允许的最大发射功率。

3）IEEE 802.15.4 标准允许 $40\times10^{-6}$ 的时钟漂移率。WirelessHART 网络是全网时间同步的，需要更精确的时钟。因此，WirelessHART 标准期望的时钟漂移率为 $10\times10^{-6}$。

4）对于 IEEE 802.15.4 MAC 层头部中的保留位或保留字节，WirelessHART 标准从未定义新的含义。WirelessHART 标准决定不要去碰这些字段，是考虑到 IEEE 802.15.4 标准在其未来的版本中可能会提供新的定义。

5）IEEE 802.15.4 标准中，所有数据类型报文的传输都需要使用 CCA。WirelessHART 报文属于 IEEE 802.15.4 的数据类型报文。但是，是否使用 CCA 在 WirelessHART 标准中是可选的。此外，WirelessHART 的确认报文不需要使用 CCA。

6）IEEE 802.15.4 标准通过在地址字段中使用不同的 PAN ID 来允许不同网络间的相互通信。而在 WirelessHART 网状网络中，通信只限于本地网络内部。

### 10.5.5 采用 IEEE 802.15.4 标准的一些额外好处

1）我们能够利用符合 IEEE 802.15.4 标准的当前和未来的商业化芯片来实现 WirelessHART 设备。一些预测认为 WirelessHART 的市场成交量比 IEEE 802.15.4 的市场成交量小两个数量级。

2）符合 IEEE 802.15.4 标准的当前和未来的商业化芯片在 MAC 层会有一些硬件方面的改善和加速。我们可以充分利用这些改善和加速。

3）我们可以使用任何符合 IEEE 802.15.4 的抓包器来读取 WirelessHART 报文。

4）然而，除非找到特征性的信息，否则抓包器无法从其他符合 IEEE 802.15.4 标准的报文中区分出 WirelessHART 报文，因为报文中没有 WirelessHART 自定义的签名字节。

### 10.5.6 信标

按照 IEEE 802.15.4 标准规定，现有网络发送出信标报文以广播该网络的存在，同时新设备监听信标报文以发现该网络和网络 ID。新设备也可以发送信标请

求报文，现有网络将用信标报文来回复。发现现有网络的 PAN ID 的唯一途径是从其信标报文中获悉。新网络在形成网络之前将主动扫描信道。新网络发送信标请求报文，其他网络将用信标报文来回复。如果设备接收到相同的 PAN ID 但是来至于不同的协调器设备地址，那么该设备就会报告 PAN 冲突。

WirelessHART 设备不支持信标。如果某个网络 ID 被 WirelessHART 网络使用，那么符合 IEEE 802.15.4 标准的网络协调器将发现不了该 WirelessHART 网络。此外，它也无法知道自已选取的信道是否是无干扰的。这意味着一个 IEEE 802.15.4 网络（如 ZigBee 网络或其他 WirelessHART 网络），可能与某个正在运行中的 WirelessHART 网络具有相同的网络 ID。于是，这两个不同网络的报文将会彼此混淆。

为了解决这个问题，我们可以使 WirelessHART 接入点具备信标的能力。目标是防止其他网状网络在任何现有 WirelessHART 网络已占用的信道上选取同样的网络 ID。值得注意的是 WirelessHART 网络通常被部署在可控的环境中，因此我们可以通过手动设置网络 ID 来避免上述问题的发生。我们在这里讨论的是一种自动的解决方案。在这种解决方案中，WirelessHART 接入点周期性地在所有信道上发送信标报文。该信标报文的发送时间间隔不需要相等，仅需要确保在一定时间间隔内在每个信道上至少发送一个信标报文。信标报文可以利用空闲时隙来发送。被选取的时隙不能被调度有 WirelessHART 网络的通信任务。

此外，WirelessHART 接入点也可以回复信标请求。接入点在发送状态之外的所有时间里都将处于侦听模式。接入点可以根据任何机制，将侦听时间分散分布在非黑名单的信道上。一旦收到信标请求报文，接入点将会在空闲时隙内回复该信标请求。

信标报文仅提供 WirelessHART 网络所使用的网络 ID，而不应该提供任何其他信息给新设备，也不应该让这些新设备尝试加入网络。

一些评论：

1）信标报文或信标回复报文可以在非空闲时隙内发送，只要在该空闲时隙还有其他信道没有被占用。为了确定某个信道在某个时隙是否被占用，我们可以利用在该时隙已被占用的信道推算出。

2）信标报文也可以在黑名单信道上发送。同时，设备还可以在黑名单信道上监听信标报文。

3）WirelessHART 网络中的其他设备也可以具有上述的信标功能。因为它们不知道全网的调度情况，所以什么时候和在哪个信道发送信标报文都必须由网络管理器统一协调。这种办法在接入点的信号无法覆盖整个 WirelessHART 网络时可能有用。

4）WirelessHART 网络在启动之前也可以使用信标机制来检测其他已经存在的网络。WirelessHART 网络可以在所有信道上监听信标报文，或在这些信道上请求

信标报文。如果另一个具有相同网络 ID 的网络正在附近运行，那么该 WirelessHART 网络可能决定不启动并向用户显示该问题、或者将该信道列入黑名单中、或者选取另一个网络 ID。

5）上述机制也可用于其他不同网络 ID 的网状网络。在启动之前，如果不同网络 ID 的网络与 WirelessHART 网络使用相同的信道，那么 WirelessHART 网络可能会要求用户采取补救措施。否则，它会自动地将这些被占用的信道列入黑名单中。

### 10.5.7 为 WirelessHART 协议栈配置 IEEE 802.15.4 协议栈

在本节中，我们通过一个小实验来简单分析如何通过实现 IEEE 802.15.4 标准来支持 WirelessHART 协议。虽然这是不实际的，但是本次练习可以让我们能更深入地比较这两个标准。

如果我们能完全访问一个 IEEE 802.15.4 物理层的软件库，那么我们应该能够直接在该软件库之上构建 WirelessHART 协议栈。这种方法的优点是可以缩短开发时间。然而，这种方法的缺点是需要更大的代码空间、更大的数据空间、可能更长的执行时间，这些都会导致电池使用寿命缩短。

大多数 IEEE 802.15.4 标准的软件产品将物理层和 MAC 层紧密地衔接在一起，只有 MAC 层的应用程序编程接口（API）是公开的。我们现在来看看如何在这类软件库之上构建 WirelessHART 协议栈。

像使用 IEEE 802.15.4 物理层的软件库一样，我们需要获得报文的抵达时间。假设无法从本地芯片的应用程序编程接口（API）获得报文的到达时间，我们可以利用从 IEEE 802.15.4 MAC 层接收到 MCPS-DATA.indication 的时间来大致计算出报文的抵达时间。当没有报文队列和 WirelessHART 设备不使用 IEEE 802.15.4 加密时，从报文接收结束至接收到 MCPS-DATA.indication 的时延可能是常量。随之而来的问题是：对于不同的硬件平台，该常量的值可能不同。因此，我们不得不测量这个常量。

表 10-3 列出了如何设置 IEEE 802.15.4 MAC 层的值以符合 WirelessHART MAC 层的要求。

**表 10-3 IEEE 802.15.4 字段中 WirelessHART 的设置值**

| IEEE 802.15.4 字段 | WirelessHART 值 | 解释 |
|---|---|---|
| phyCCAMode | 2 | 仅用于载波检测 |
| phyCurrentChannel | 变量 | 在每个时隙的开始被设置 |
| macMaxCSMABackoffs | 0 | 禁用随机退避机制 |

（续）

| IEEE 802.15.4 字段 | WirelessHART 值 | 解 释 |
|---|---|---|
| macMinBE | 0 | 禁用随机退避机制 |
| MAC payload | <102 | 否则，帧版本号将被设置为 1 |
| macBeaconOrder | 15 | 禁用活跃信标帧 |
| macSuperframeOrder | 15 | 禁用活跃信标帧 |
| macGTSPermit | FALSE | 消除随意信标帧的影响 |
| macAssociationPermit | FALSE | 消除随意信标帧的影响 |
| PANCoordinator in MLME-START. request | FALSE | 不充当协调器 |
| macDSN | ASN 的最低有效字节 | 每次都需要被设置 |
| macSecurityEnabled | FALSE | 非 IEEE 802.15.4 MAC 层加密 |
| MLME-RX-ENABLE. request | FALSE（每当无通信时） | — |
| macMaxFrameRetries | 0 | WirelessHART 自己重试 |
| macPromiscuousMode | FALSE | — |
| macRxOnWhenIdle | FALSE | 仅需在设定的时间侦听以节省能量 |

## 10.6 共存

在本小节中，我们来分析附近的其他无线网络对 WirelessHART 网络的影响，还将讨论 WirelessHART 网络如何适应其他网络的存在以及它如何影响其他网络。

在 10.5.6 节中，我们已经谈到如何积极主动地通过信标机制来实现共存。换句话说，WirelessHART 网络在形成之初可以有意识地避免与现有网络的相互干扰。在 9.10 节中，我们也谈到了敌对者如何能主动地扰乱一个 WirelessHART 网络。在本节中，我们关注被动式共存，即多个无线网络如何在一个现有环境中平和的共存。

两个无线射频信号的载波频率相距遥远，那么这两个信号将不会互相干扰。例如，如果你正在收听一个电台节目，你并不关心什么时候打开电灯。无线传输被中断的方式有两种。一种方式是附近存在相近频率的干扰信号。这样，干扰信号会扰乱当前的期望信号。当这种情况时，干扰信号并不需要很强。另一种方式是使用蛮力，即干扰信号的能量水平足够高以至于接收方无法容易地接收到发给自己的无线信号。微波炉就是一个很好的例子。微波炉在运行时会发出强大的电磁波，导致附近所有的无线设备都会受到影响。

WirelessHART 网络工作在 2.4GHz 频段。通常情况下，WirelessHART 网络应该可以与其他频段的无线网络和平共存。我们接下来讨论 2.4GHz 频段的其他网络。

2.4GHz 频段的免费使用引发了大量非常先进的无线技术。我们已经看到了许多基于这个频段的标准和产品。不幸的后果是该频段变得越来越拥挤，同时共存问题也变得越来越重要。

### 10.6.1 IEEE 802.15.4 标准

对无线网络最有效的干扰是来自于其同类型的其他网络。WirelessHART 标准被定义成允许多个 WirelessHART 网络共存，其中每个 WirelessHART 网络必须有一个唯一的网络 ID。如果两个 WirelessHART 网络在同一物理信道上同时发送数据，那么两者的数据传输都将失败。然而，由于 WirelessHART 网络低数据率的本性和伪随机跳信道技术，这样的冲突通常是很少见的。此外，WirelessHART 网络中建立的重传机制可用于处理传输失败。人为干预，也可以减少冲突。例如，我们可以给不同的 WirelessHART 网络分配不同的物理信道。更具挑战性的是我们可以协调调度多个无线网络。

以下是针对两个相互干扰的 IEEE 802.15.4 报文的一些观察结果：

1）由于 IEEE 802.15.4 标准使用了直接序列扩频（DSSS）技术所以两个 IEEE 802.15.4 报文不能在同一物理通道上同时发送。

2）如果两个 IEEE 802.15.4 网络使用不同的物理信道，那么它们可以相互共存；

3）如果两个 IEEE 802.15.4 网络使用相同的物理信道，那么由于报文冲突，它们无法很好地共存；

4）IEEE 802.15.4 标准定义的 16 个信道可以被同时使用，而不像 IEEE 802.11b™标准中 16 个信道最多只有 3 个信道可以被同时使用。

WirelessHART 标准是基于 IEEE 802.15.4 标准的。同时，一些其他的网络协议（如著名的 ZigBee™协议）也是基于 IEEE 802.15.4 标准的。因而，这两者间的共存问题吸引了很多关注。当 ZigBee 网络部署在 WirelesHART 网络附近时，人们通常认为 ZigBee 网络成功通信的机会更高。

ZigBee 网络占用一个物理信道。ZigBee PRO 标准附加了额外功能用来切换正在运行的网络的信道。在任何情况下，ZigBee 网络对 WirelessHART 网络的干扰是有限的，这是因为 WirelessHART 网络采用了跳信道技术。同样的，由于单一的 ZigBee 信道只会被 WirelessHART 网络随机的访问，所以 WirelessHART 网络对 ZigBee 网络的干扰也是有限的。这两种网络中的设备都可能会接收到对方网络的报文。如果 ZigBee 网络的 PAN ID 与 WirelessHART 网络的网络 ID 不同，那么设备都会简单地丢弃掉对方的报文。然而，WirelessHART 网络和 ZigBee 网络并不能自动

地发现对方的存在，以及发现对方的网络 ID。这个问题已经在 10.5.6 小节讨论过了。因此，现场工程师必须确保它们使用不同的网络 ID。

### 10.6.2　IEEE 802.11 标准

到目前为止，2.4GHz 频段中最突出的标准是 IEEE 802.11a/b/g/n™，也称为 Wi-Fi。Wi-Fi 主要部署于住宅和办公室环境中，同时在过程工业环境中也取得了一些进展。一个事实是 2.4G 频段变得越来越拥挤。另一个事实是该领域的人们都意识到了这个问题。

Wi-Fi 技术占用更宽的物理信道带宽和使用更高的发射功率。通常，Wi-Fi 网络更容易影响到 WirelessHART 网络，而不是被 WirelessHART 网络影响。IEEE 802.15.4 标准中附件 E 提供了一些 IEEE 802.15.4 标准与其他 IEEE 标准或 IEEE 推荐标准共存的权威性分析。这里列举了其中的一些重点：

1）对于非跳频系统，大的频率差别允许近距离共存（小于 2m 的距离）。而小的频率差别，或同频率干扰，就要求几十米的远距离共存。发射功率水平是同信道干扰的主导因素。

2）干扰信号对期望信号的影响可被假定为与在相同带宽里的加性高斯白噪声（AWGN）相似。

3）只要 IEEE 802.15.4 网络在某个信道上使用了独特的扩频技术，那么其他同频的无线信号可被简单地认为是噪声。

4）4 个 IEEE 802.15.4 信道存在于三个 IEEE 802.11b 信道之间的保护地带。在北美地区，这 4 个信道的信道编号（$n$）分别为 15、20、25、26。在欧洲，这 4 个信道的信道编号（$n$）分别为 15、16、21、22。虽然 IEEE 802.11b 信号在这些保护地带上的功率不一定为零，但是要比信道内的能量低。如果 IEEE 802.15.4 网络运行于这些信道上，那么将能最大限度地减少 IEEE 802.15.4 网络与 IEEE 802.11b 网络之间的干扰。IEEE 802.11n 占用更宽的信道带宽。每个 IEEE 802.11n 信道的频率范围相当于两个 IEEE 802.11b 信道的频率范围。由于 IEEE 802.11n 扩展了其信道带宽，因此这 4 个 IEEE 802.15.4 信道也变得不再安全。

CCA 能量阈值的提高可以改善信号在有同频干扰信道中的传输。干扰频率将不会损害解码太多。CCA 能量阈值设置太低将引起不必要的 CCA 检测失败和终止可能的成功传输。

以上所有分析都适用于 WirelessHART 网络。同时，WirelessHART 标准提供了许多其他的共存方法：跳信道、重试传、多路径、黑名单等。

ZigBee 和 Wi-Fi 网络间的共存已有了大量的研究结果。这些研究结果大体上都是有效的。针对 WirelessHART 与 Wi-Fi 网络之间的共存分析，一种有效的方法是将 WirelessHART 等同成具有跳信道功能的 ZigBee 网络，然后再分析这类 ZigBee 网

络与 Wi-Fi 网络之间的共存。

### 10.6.3 其他标准

由于许多其他无线网络采用了与 WirelessHART 不同的调制技术，所以它们的信号对 WirelessHART 设备不会造成太大的影响，只会简单地以白噪声的形式出现。它们干扰 WirelessHART 网络或被 WirelessHART 网络干扰的主要因素是彼此间的发射功率的大小。这些无线网络包括 Bluetooth™（蓝牙）、Wibree™、RFID、UWB、WiMAX™网络、对讲机、手机、基站、中继器、专用收音机等。

（1）Bluetooth（蓝牙） 蓝牙是一个不断发展的技术，其最新的版本是 3.0 版。该最新版本可能包括 IEEE 802.11 标准或 UWB。在这里，我们使用蓝牙 2.0 版本作为参考。

蓝牙设备也运行在 2.4GHz 的 ISM 无线电频段。它支持时隙和跳信道。然而，它的信道远比 IEEE 802.15.4 的信道窄。蓝牙协议将整个 2.4GHz ISM 频段分为 79 个信道（每个信道带宽为 1MHz），并以高达 1600 次/s 的速度切换信道。蓝牙设备和 WirelessHART 设备之间的干扰可以被彼此认为是噪声，并且可以被忽略不计。

（2）RFID RFID 即射频识别技术。其主要用途是为 RFID 阅读器识别出附着在某些物体上的 RFID 标签。RFID 的无线通信方式是点对点的，可使用包括 2.4GHz 在内的任何无线电频段。RFID 的应用和使用模式与 WirelessHART 网络完全不同。

（3）UWB UWB 即超宽带技术。UWB 技术同时占用极宽的无线电频谱用来传输数据。因此，接收到 UWB 信号的 WirelessHART 设备会将其认为是白噪声信号。许多标准（如 WiMAX 和 IEEE 802.15.4a 标准）都采用了 UWB 技术。

### 10.6.4 共存测试场景

2.4GHz ISM 频段的共存测试已经有许多了。一个共存测试可能包括以下项目：

1）信号接收强度。

2）传输范围。

3）作为干扰源或被干扰者的测试目标。

4）流量模型。

5）信道的选取。

6）帧长。

7）天线增益。

8）路径衰落。

## 10.7 HART及其他现场总线标准

多年来，过程控制系统经历了几代的发展。现场总线是过程控制系统中一个重要的里程碑。现场总线通过总线网络将现场设备连接到上位机，而不是每个设备各自连接到上位机。现场总线是工业级的，它们有更多的限制和要求。一些流行的网络协议（如以太网）不能直接用于过程工业现场，除非它是经过改进的。随着设备的网络化，许多新功能被开发出来。例如，一些现场总线支持现场控制（control-in-the-field）。在不需要上位机参与的情况下，运行在设备中的控制模块就可以完成一个控制回路，这即为现场控制（control-in-the-field）。现场总线也激活了许多诊断和维护功能，这样能为用户节省大量的成本。许多不同的现场总线协议也已被开发出来了，如Foundation Fieldbus，Profibus，DeviceNet™，Modbus等。

HART通信协议是这些现场总线之一。在最初的设计中，HART通信协议利用现有的4～20mA双绞线提供维护功能。其他现场总线通常要求更换以前的非现场总线控制系统，但是HART总线不是用来取代这些非现场总线控制系统的，而是建立在这些非现场总线控制系统之上的。用HART设备取代传统的设备后，在无需其他硬件改造的情况下，上位机突然就能获得很多设备信息。HART标准允许继续按旧的方式处理过程数据。由于HART标准的简单和逐步演化的特性，它在世界上拥有最大的现场安装量。

无线代表着仍在进行中的另一代。WirelessHART标准绝不是定义一个全新的无线总线协议，而是通过在HART标准上扩展无线功能来延续它的传统。WirelessHART网络是一个拥有最新无线技术的、真正意义上的网状网络。与此同时，WirelessHART网络顺利地继承了有线HART网络的特性。这样，大量的有线HART系统和设备都可以轻松地转变到无线模式。目前，我们还没有任何关于其他现场总线转变到无线模式的重要消息。

随着WirelessHART网络的使用，过程和控制数据可以不再通过模拟的4～20mA线路来传输。然而，这样就会出现一个奇怪的现象：现场驱动器对每个发给自己的数据报文都要回送一个响应报文，例如在控制回路中，周期性输出数据被嵌入到命令79中发送给执行器，而命令79要求一个响应报文。实际上，依据过程控制的习惯做法，周期性的数据并不需要响应。

## 10.8 WirelessHART标准应用范围

WirelessHART标准从一开始就设置自己的范围。它并不打算成为一个无所不包的无线标准。WirelessHART网络是一种针对流程控制行业的低功耗、低数据率

的网状网络。虽然 WirelessHART 技术使其能够适用到一些非目标应用领域，但是 WirelessHART 标准并不打算应用到任何超过其目标范畴的应用领域。WirelessHART 标准并不适用于数据传输频率低到几个毫秒或毫秒以下水平的工业制造领域。

WirelessHART 标准没有明确规定 WirelessHART 网状网络之外的事物是如何工作的。WirelessHART 标准中一个显而易见的默认是没有规范网关和上位机之间的骨干传输。你也将不会在 HART 标准里看到用于大数据传输的无线骨干网。

WirelessHART 标准指明了网关或网络管理器的一些规则，但是并没有规定如何实现网关或网络管理器。它并没有强制规定网络管理器如何配置网络。这样的后果是：如果存在一个坏的网络管理器实现，则 WirelessHART 标准可能会被无辜地指责其效率低下；另一方面，一个优秀的网络管理器可以构建出一个极好的 WirelessHART 网络。

## 10.9　安全和可靠性

当人们谈论无线的时候，首先引起关注的是安全（McCluer 2003）。这是可以理解的。毕竟，任何人在任何地方都可以获得无线信号。不过，从技术角度来看，真正值得关注的是可靠性。最新的加密技术既可以适用于有线领域，也可以适用于无线领域。应用在无线系统中的 CCM*算法并不会更容易被攻破。无线网络中的安全可以像任何其他网络一样好。无线网络可能不比有线网络更安全，但是无线网络面临的安全问题也同样存在于有线网络里。

WirelessHART 标准中的 CCM*算法来源于 IEEE 802.15.4 标准中的 CCM*算法。IEEE 802.15.4 标准中的 CCM*算法是基于 AES 算法的。该 AES 算法是由美国国家标准和技术局（National Institute of Standards and Technology，NIST）制定的，并作为联邦信息处理标准（Federal Information Processing Standard，FIPS）——FIPS 197 发布的。FIPS 197 兼容 NIST FIPS 140-2，后者能够满足一些政府机关和公司的要求。

WirelessHART 标准没有规定 WirelessHART 网络与上位机或其他外部应用程序之间的通信。所以，与这部分相关的安全问题超出了 WirelessHART 标准的范畴，因此也不应该以此来批评 WirelessHART 标准。

WirelessHART 网络还可以定义设备白名单或设备黑名单。白名单中的设备可被允许加入该网络，而黑名单中的设备不被允许加入该网络。如果定义了这两种名单，那么在白名单上而不是黑名单上的设备才能被允许入网。这里的设备黑名单与信道黑名单无关。

在 WirelessHART 网络中，安全管理器管理着所有的密钥，所以安全管理器本

身必须要确保是安全的。安全管理器与网络管理器之间的通信位于 WirelessHART 网络之外，也必须要确保安全，可以使用安全领域最好和最新的技术来确保其安全。WirelessHART 网络设备中的所有密钥都只是可更改的。

相比于有线通信，无线通信的一个主要不足是可靠性差。环境噪声、反射、路径衰落、移动性等都是无线通信固有的问题。WirelessHART 标准采用了一系列最新技术来克服这个不足之处。许多术语被用来描述可靠性的某一方面，如可用性、生存能力、相关性、完整性、安全、可执行性等。

WirelessHART 标准利用多种复用技术来保证其通信具有很高的可靠性：

（1）时分复用　所有非广播报文都要求接收方在同一时隙内对其进行确认。当传输失败的时候，重传机制将会被启动。

（2）空间（路径）复用　WirelessHART 网络的拓扑结构是网状的。每对端到端的通信必须有两条以上的可用路径。

（3）频率复用　WirelessHART 标准提供了基于 16 个信道的跳信道技术。

（4）编码和极性　WirelessHART 标准采用了 IEEE 802.15.4 标准。IEEE 802.15.4 标准的编码和调制方式是合理可靠的。我们期望其在未来版本中能得到进一步加强。

## 10.10 WirelsssHART 技术的使用极为简单

没有，就像回答类似问题：“我需要知道汽车的所有机械结构才可以开车吗?”。许多用户已经反馈 WirelessHART 的使用是多么的容易。用户只需要收到货物、拆包、安装并打开电源。于是，整个 WirelessHART 网络就自动形成了。

WirelessHART 标准非常重视使用的简便性。例如，正如我们在第 10.4 节中讨论的，WirelessHART 标准并不需要高技术的现场勘查。

# 第三部分　WirelessHART 实践

在这一部分，我们来关注 WirelesHART 标准的使用。

第 11 章介绍来自于 HART 通信基金会的 WirelessHART 测试和诊断工具：Wi-Analys 和 Wi-HTest。本章还将会详细描述本书作者领导开发的 Wi-HTest。

第 12 章提议一些方式以便快速地将传统有线 HART 设备接入到无线世界。

第 13 章针对 WirelessHART 产品开发提出一些建议。这些建议都是来源于本书作者自己的开发经验。

第 14 章给出建议如何最好地使用 WirelessHART 设备和网络。

# 第 11 章　测试和诊断工具

摘要：WirelessHART 一致性测试需要测试规范和测试工具。WirelessHART 测试工具包括 Wi-HTest 工具、Wi-Analys 工具和一个后期处理套件。该后期处理套件可用于分析 Wi-Analys 工具捕获的报文，还可用于总结测试结果并产生最终的一致性报告。Wi-Analys 工具是一个被动的抓包器，它能捕获 WirelessHART 报文以供分析。Wi-HTest 工具提供了一个网络管理、网关、接入点脚本执行和通信功能的组合。Wi-HTest 工具把被测设备加入到测试系统中，然后执行各种测试脚本并允许测试中引入各种扰动。Wi-Analys 工具捕获测试系统和被测设备之间的网络通信，并将其发送给后期处理工具用于评估。我们有超过 200 个的包括有线和无线的 Wi-HTest 测试脚本。这些 Wi-HTest 测试脚本包含了数以百计的不同测试场景和数以千计的不同故障点。每一个测试脚本意味着一次 Wi-HTest 工具的执行。为了更好地管理整个测试过程，Wi-HTest 测试脚本还包含了一些发给 Wi-Analys 工具的特殊报文。

符合标准是供应商在市场上成功的关键。这可以帮助它们避免昂贵的产品返工和降低技术支持的成本。为了确保 HART 产品（包括 WirelessHART 设备）符合标准，HCF 从 1995 年起启动了一个严格的质量保证计划，即所有的 HART 设备都必须进行彻底的测试并在 HCF 注册。作为这个计划的一部分，HCF 为 HART 标准制定了具体的测试规范并开发了相关的测试工具。在 WirelessHART 标准发布的同时，HCF 也发布了 Wi-HTest 测试工具。Wi-HTest 测试工具是对原有 HTest 测试工具的扩展，它用于支持 WirelessHART 产品的质量保证，特别是时序一致性测试。HCF 同时还发布了一个叫做 Wi-Analys 工具的抓包器，该抓包器用于实时监测 WirelessHART 网络。HCF 还将发布一个后期处理套件用来分析 Wi-Analys 工具捕获的报文并产生最终的一致性报告。所有这三个工具组合在一起为 WirelessHART 设备提供了一个完整的一致性检测环境。

Wi-Analys 和 Wi-HTest 工具还可以有其他的用途，其范围可以从供应商的开发到客户的设备部署。而且，Wi-Analys 和 Wi-HTest 工具各自都可以被当做一个独立的工具来使用。

## 11.1　Wi-Analys 工具

Wi-Analys 工具是一种符合标准 IEEE 802.15.4 的接收器，也是一个针对 Wire-

lessHART 报文的抓包器。它的产品名称是 HCF_ KIT-190™。Wi-Analys 工具可以被用来对 WirelessHART 设备进行全面的测试，并分析这些设备发出的报文。它还可以同时在 16 个信道上侦听并捕获所有符合 IEEE 802.15.4 标准的报文。如果被捕获的报文是一个合法的 WirelessHART 报文，WirelessHART 报文中每个协议层的字段，从物理层一直到应用层，都可以被提取并在 Wi-Analys 中显示。

Wi-Analys 工具由一个无线电接收盒和在 PC 上运行的软件套件组成。

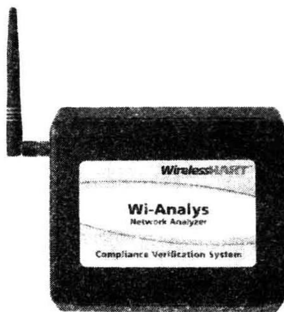



图 11-1 Wi-Analys 工具

图 11-1 是一个无线电接收盒。它只有一个物理天线用来侦听所有 16 个物理信道。每一个接收到的报文都会根据内部的时钟被给予一个时间戳。时钟运行在精确度为 $10\times10^{-6}$的晶体上。无线电接收盒通过 USB 电缆连接到 Windows 工作站。

PC 上的软件可以显示各种捕获到的报文。Wi-Analys 工具可以实时地捕捉报文或者重播保存的日志文件。对于实时的报文，它最大的捕捉速度可达 1000 个报文/s。所有 16 个信道上的报文都可以被同时捕获。Wi-Analys 工具可以显示某些指定报文的指定字段，还可以显示收集到的报文的统计信息。

Wi-Analys 工具还有很多方法来过滤报文使其不被显示。用户可以选择需要显示的报文类型。对我们最有用的过滤器是网络 ID 过滤器和通告报文过滤器。很多时候，我们的开发环境中会有一个以上的 WirelessHART 网络。因此，过滤掉不属于我们网络的报文可以帮助我们专注于当前所做的工作。此外，当我们正在开发 WirelessHART 系统时，Wi-Analys 工具还会捕获到大量的通告报文。通过过滤掉这些通告报文包，我们可以专注于所关心的通信报文。

Wi-Analys 工具接受安全密钥的方式有两种：一种方式是用户输入，另一种方式是对 Wi-HTest 工具发送出来的报文进行智能解码。Wi-HTest 工具发送出来的报文既有可能是发给 Wi-Analys 工具的配置报文，也有可能是发给某个设备用于配置密钥的报文。Wi-Analys 工具将使用它拥有的密钥来对这些报文进行验证或解密。解密失败的报文将用不同的颜色表示。图 11-2 是 Wi-Analys 软件显示窗口的截屏。

表 11-1 列出了 Wi-Analys 工具中定义的数据字段。

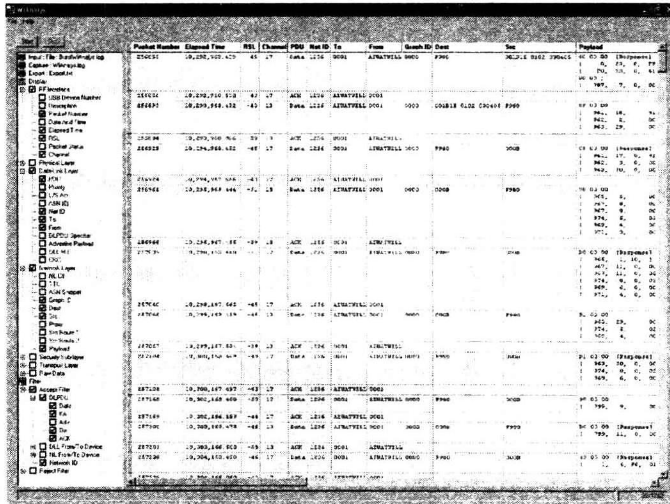


图 11-2 Wi-Analys 截屏

表 11-1 Wi-Analys 工具中定义的数据字段

| 协议层 | 名 字 | 解 释 | 例子：入网响应报文 |
|---|---|---|---|
| RF 接口 | USB Device Number | 无线电接收盒序列号 | 115077 |
| | Description | IEEE 802.15.4 报文类型 | 802.15.4-数据 |
| | Packet Number | — | 680 |
| | Date And Time | 原始时间戳 | 2009-09-20 03：01：57.031 |
| | Elapsed Time | 准确时间戳 | 348，453.681 |
| | RSL | 接收信号强度 | -50 |
| | Packet Status | 报文状态 | 0x0000 |
| | Channel | 物理信道 | 11 |
| 物理层 | Byte Count | 字节数 | 110 |
| 数据链路层 | PDU | WirelessHART 报文类型 | 数据 |
| | Priority | WirelessHART 报文优先级 | 命令 |
| | L/S Adr | 长短地址 | 88 |
| | ASN (0) | 最低位绝对时隙数字节（序列号） | B0 |
| | Net ID | 网络 ID | 1236 |
| | To | 数据链路层目标地址 | 0005 |
| | From | 数据链路层源地址 | 0001 |
| | DLPDU Specifier | | 37 |

（续）

| 协议层 | 名　字 | 解　释 | 例子：入网响应报文 |
|---|---|---|---|
| 数据链路层 | Advertise Payload | 如果是广播报文 | — |
| | DLL MIC | 数据链路层 MIC | CB2A0763 |
| | CRC | — | FBEB |
| 网络层 | NL Ctl | 控制字节 | 85 |
| | TTL | — | 7E |
| | ASN Snippet | — | 684C |
| | Graph ID | — | 0000 |
| | Dest | 网络层目标地址 | 001B1E2659000000 |
| | Src | 网络层源地址 | F980 |
| | Proxy | 代理地址 | 0001 |
| | Src Route 1 | 源路由表-1 | 000100050004FFFF |
| | Src Route 2 | 源路由表-2 | — |
| 应用层 | Payload | 网络层有效载荷 | 8F 00 00 * [ 961, 16, 0D 32 23 40 7E 44 48 5D 65 D9 B8 DB 0B 92 C1 B9 ] * [ 962, 2, 00 04 ] * [ 963, 29, 00 F9 80 F9 80 00 00 01 00 00 00 00 9B 9D 57 11 C4 5C D4 CA 2A 10 07 DE 5C D2 28 01 00 ] |
| 安全层 | SL Ctl | 安全控制字节 | 加入 |
| | SL Cnt | 随机数计数器 | 0000087C |
| | SL MIC | 网络层 MIC | 37DE8837 |
| 传输层 | TL Ctl | 传输层控制字节 | 8F |
| | TL Status | 设备状态 | 00 |
| | TL ExStatus | 扩展设备状态 | 00 |
| 原始数据 | Cipher Text | 原始报文字节流。第一个字节是流的长度 | 6E4188…. F6C4…. CB2A0763FBEB |
| | Clear Text | 网络层有效载荷解码的报文字节流 | 6E4188…. F980…. CB2A0763FBEB |

## 11.2　Wi-HTest 工具

作为 WirelessHART 测试系统的一部分，Wi-HTest 工具被设计成与 HTest 工具

以及 Wi-Analys 工具协同工作来验证 WirelessHART 设备的标准一致性。它的产品名称是 HCF_ KIT-193™。根据 HCF 的定义：

无线测试系统对 WirelessHART 设备的开发和标准一致性测试至关重要。制造商在提交自己的设备给 HCF 进行注册之前，必须使用该测试系统对自己的设备进行测试。

HCF 使用 HTest 工具来测试有线 HART 产品的标准一致性。HTest 工具是一个带有 HART 调制解调器的、在 PC 上运行的、通用的 HART 主程序。HTest 工具使用一个叫做 CINT（root. cern. ch/twiki/bin/view/ROOT/CINT）的简单的解释性脚本语言来建立、发送、接收和显示符合 HART 标准的报文。HTest 通过检查响应报文的正确性来验证被测设备的标准一致性。然而，伴随着 WirelessHART 标准的发布和 WirelessHART 设备在市场上的迅速推广，HCF 必须对 HTest 工具进行扩展以支持对各种无线命令的测试，并确保 WirelessHART 设备的标准一致性。

作为一个专门为无线实时通信协议设计的测试套件，Wi-HTest 工具有两个固有的功能。第一，它能够实时地产生测试报文，并通过 IEEE 802. 15. 4 物理层在精确的时间点上发送给被测设备。第二，Wi-HTest 工具可以捕获从被测设备发回的响应报文以及精确的接收时间。这两个功能使得 Wi-HTest 工具不仅可以检查响应报文的正确性，同时还可以验证响应时间的精确性。

Wi-HTest 工具旨在自动地执行由 WirelessHART 测试规范所定义的各种测试案例。更具体地说，Wi-HTest 工具提供了各种各样测试案例来对被测设备进行操作。这些测试案例大致可以分为两个不同的测试场景：设备加入网络过程场景和正常的数据通信场景。在设备加入网络过程场景中，Wi-HTest 工具与被测设备之间通过一系列报文交换来进行交互，并验证被测设备是否能够成功地加入 WirelessHART 网络；在正常的数据通信场景中，Wi-HTest 工具通过执行特定的测试脚本来向被测设备发送正确的报文，或者发送含有错误信息的报文。通过检查被测设备在收到正确或者错误报文后的响应行为，我们就可以评估出被测设备的标准一致性。

### 11. 2. 1 WirelessHART 测试规范和测试脚本

开发者当开发一个遵循 WirelessHART 标准的现场设备时，需要完成各种非正式的随机测试和正式测试。HCF 通过为开发者提供一个测试规范来简化这些测试工作。在产品发布和在 HCF 进行产品登记之前，生产厂商必须完成这个测试规范以及提交相应的测试报告。这个测试规范提供了明确的测试要求，并减少了生产厂商必须制定的测试计划的数量。它们可用于在早期的发展中检查设备实现的功能，并作为回归测试程序中很重要的一个部分来对现场设备进行维护和加强。此外，这个测试规范对 WirelessHART 标准中定义含糊之处进行了更明确的说明，并且对 WirelessHART 标准拥有最终的解释权。

这个测试规范使用了准黑盒的方法来确认被测设备的标准一致性。一套完整的 WirelessHART 测试包括以下五个阶段，每个阶段都包含了多个顺序执行的测试描述。

1）开机测试。

2）单设备测试。

3）多设备测试。

4）多信道选择测试。

5）负荷测试。

开机测试通过维护端口或者是无线连接来测试被测设备内部已经实现的命令集。这些测试还可以配置被测设备，通过把它们设置成初始化状态来测试它们加入某个 WirelessHART 网络的过程。

在成功完成开机测试之后，单设备测试则侧重于被测设备直接和网络管理器以及网关交互的测试环境。这一系列的测试表明该无线现场设备可以正确请求加入到无线网络，接受包括延迟执行命令在内的各种网络操作以及与对端设备的时间同步。和单设备测试不同，多设备测试表明被测设备可以与多个其他设备进行交互，并从接收到的报文中得到这些设备的信息。

多信道选择测试是对多设备测试的一个扩展。它检查被测设备能否在多个可选的信道中作出正确的响应。

最后，负荷测试把前面的各种测试组合在一起形成一个随机的测试序列。负荷测试展示了在模拟现场环境中对被测设备的连续操作。这个测试阶段的主要目的是检查被测设备是否能够在真实的现场工厂环境中进行可靠的通信。

依据 WirelessHART 测试规范，我们为不同测试阶段的每个测试案例编写了相应的测试脚本。测试脚本是一个短小精悍的测试程序。作为 Wi-HTest 工具的输入，测试脚本被用来建立测试环境、产生适当的测试报文、并执行标准一致性测试。通常，一个测试脚本由两部分组成：测试配置和测试主体。测试配置部分负责初始化网络管理器、网关及各种测试参数。测试主体则由一系列小的测试步骤组成。每个测试步骤通过调用 Wi-HTest 工具提供的程序库来生成所需要的 WirelessHART 报文。

## 11.2.2 Wi-HTest 架构

### 11.2.2.1 概述

WirelessHART 标准是一个工业级的实时协议。我们计划使用 Wi-HTest 测试套件来验证被测设备的数据正确性和时序一致性。HTest 工具用于有线 HART 设备的一致性测试，而 Wi-HTest 工具支持针对无线命令的测试，也是对 HTest 工具的一个扩展。

Wi-HTest 工具包括了两个组件：Wi-HTest 上位机和 RF 接口。图 11-3 展示了这个工具。图中左边的盒子是一个运行 Ubuntu Linux 系统的小型个人计算机。图中右边的盒子是 RF 接口。图 11-4 描述了 Wi-HTest 测试套件的高层架构。

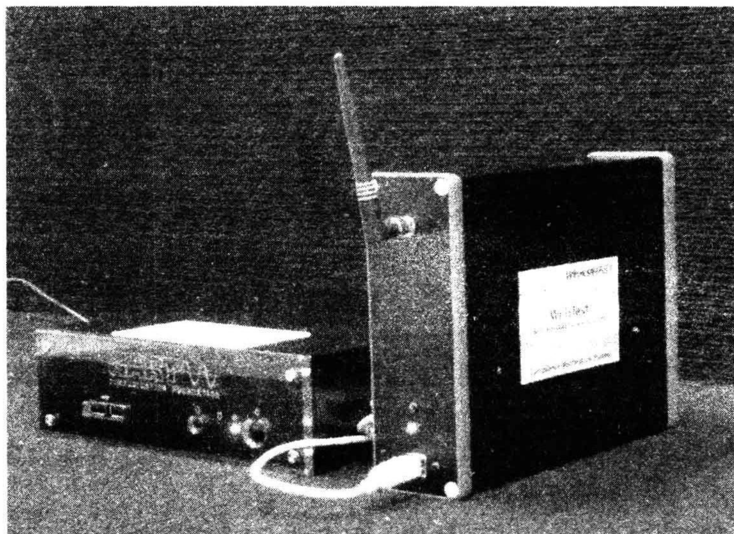


图 11-3 Wi-HTest 工具

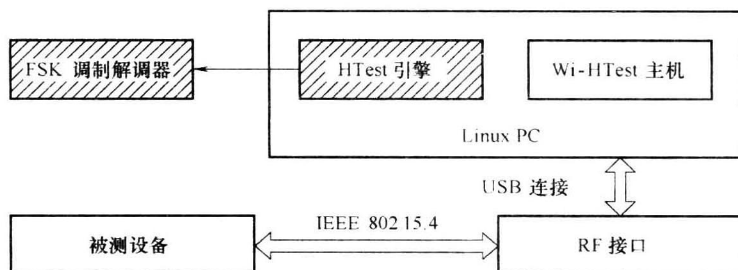



图 11-4 Wi-HTest 高层架构

Wi-HTest 上位机负责整体控制和执行输入的测试脚本。根据测试脚本的具体要求，Wi-HTest 上位机将产生正确的报文，或在报文的有效载荷或各层头部中加入错误的信息。然后，Wi-HTest 上位机再将这些报文通过 RF 接口发送给被测设备。RF 接口内部运行有一个实时的嵌入式 WirelessHART 伪协议栈。RF 接口通过板载的无线收发器来与被测设备之间进行低层的、实时性通信。从被测设备发回的响应报文将被返回给 Wi-HTest 上位机，同时 Wi-Analys 工具也会捕获这些响应报文并用于后期处理。最后，后期处理套件将读取 Wi-Analys 工具记录的日志文件

（尤其是响应报文的时序信息），并生成针对被测设备的一致性报告。以下章节将详细讨论 Wi-HTest 工具的系统设计。

#### 11.2.2.2　上位机架构

Wi-HTest 上位机运行在基于 Linux 系统的小型 PC 上。它由三个模块组成：RF 接口驱动程序，网络层库以及 Wi-HTest 引擎。图 11-5 给出了 Wi-HTest 上位机的架构。这些模块紧密合作来实现以下功能：

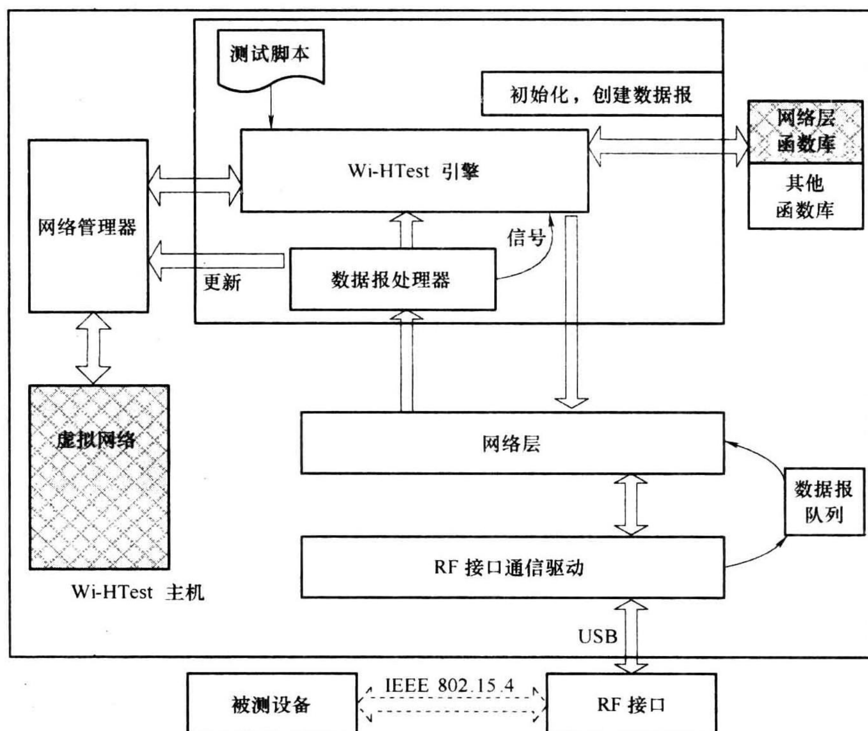



图 11-5　Wi-HTest 上位机架构

1）读取输入的测试脚本，并建立相应的设备和测试环境。

2）根据测试脚本的要求，产生相应的命令，然后将该命令作为有效载荷并加上适当的网络层头部。如果必要的话，还需要在报文中加入指定的错误信息并进一步告知数据链路层如何修改数据链路层头部。

3）将控制信息和报文发送给数据链路层并等待被测设备的响应。

每个模块的实现细节描述如下：

1. RF 接口驱动

Wi-HTest 上位机和 RF 接口通过 USB 相连（见图 11-4）。它们之间使用一个简

单的私有协议进行通信。该协议提供了基本的成帧功能，如前同步码、分隔符、帧控制和 CRC 错误检测。

Wi-HTest 上位机和 RF 接口之间的 USB 电缆上传输着三种类型的命令：①由 Wi-HTest 上位机发出的对 RF 接口进行配置的命令（类型Ⅰ）；②在 Wi-HTest 上位机和 RF 接口之间传递报文的命令（类型Ⅱ）；③RF 接口发给 Wi-HTest 上位机用来更新它的某些数据结构的命令。基本上，类型Ⅰ命令大部分是 WirelessHART 命令。命令 965 就是其中的一个例子，它是用来配置 RF 接口上的超帧信息。目前，命令 64513 是唯一一个被定义了的类型Ⅱ命令。命令 64513 用来表示标准的网络层到数据链路层的数据请求，或者表示数据链路层到网络层的数据指示。目前我们也只有一个类型Ⅲ的命令，即命令 64518。RF 接口使用命令 64518 来更新其在 Wi-HTest 上位机中的 ASN 信息。这为 Wi-HTest 上位机提供了一个粗略的 ASN 信息，以用于填补网络层头部中的 ASN 片段字段。更多的类型Ⅲ命令将会被引入，来为上位机和 RF 接口之间提供数据的共享。

帧计数器字段被用来保证 Wi-HTest 上位机和 RF 接口之间的可靠通信。通信双方的端节点各自保存了两个帧计数器，一个用于自己，一个用于对方的端节点。每当设备发送一个帧时，其自身的帧计数器将会加 1。每当设备接收到一个帧时，它将把收到的帧中的计数器和自己为对方保存的帧计数器进行比较。如果两者相同，那么收到的帧是所期望的。否则，收到的帧将会被自动丢弃掉。每当一个正确的帧被收到时，接收方将针对发送方的帧计数器加 1。

2. Wi-HTest 上位机上的网络层

Wi-HTest 上位机上的网络层被构建成一个函数库和一个独立的接收线程。网络层函数库提供各种可调用的函数，用以创建或者修改数据的有效载荷和报文头部；而接收线程处理从 MAC 层收到的响应报文或其他未经请求的报文。

网络层被从 RF 接口中剥离出来并放在 Wi-HTest 上位机上主要基于以下三个原因：①与 MAC 层相比，网络层的大部分操作并不是时间关键的。考虑到有限的内存和处理器资源，以及 RF 接口上严格的时序要求，把网络层放在 Wi-HTest 上位机上可以节省更多的资源用来实现 RF 接口上的 Wi-HTest 专用模块。②网络层放在 Wi-HTest 上位机上可以更直接、更方便地在测试脚本中修改 WirelessHART 命令的有效载荷、网络层头部、甚至是 MAC 层头部。在 Wi-HTest 上位机上，这些操作现在可以直接通过调用相应的函数来实现。否则，测试脚本必须把这些控制信息通过各种接口消息来传达给 RF 接口。③将网络层放在上位机上为我们提供了模拟虚拟设备和形成虚拟网络的可能性和灵活性。

网络层函数库提供了许多有用的调用函数来支持各种网络操作。例如，基于给定的参数，一组函数可以被用来构建网络层头部，而另一组函数可以用于解析现有的网络层报文。该函数库还包含了各种函数，这些函数可以用于网络层的初始化和

配置、创建接口消息、加密解密和验证网络层的报文以及维护网络层的各种通信表。

在每个测试案例中，当一个传输命令从测试脚本中读取之后，Wi-HTest 上位机中的测试引擎将会通过调用网络层函数库中相应的函数来创建正确的或是经过故意修改的网络层报文，并把这些网络层报文发送到 RF 接口；前面提到的独立的接收线程将一直监听接收报文队列，并通过调用相应的函数来处理不同类型的报文。如果接收到的报文是正在被等待的一个响应报文，那么它将被保存在一个共享的缓冲区内，并唤醒测试引擎来进行处理。在其他情况下，报文将被丢弃，或用来更新相关的数据结构。这类报文的一个例子是由每个设备生成的周期性的邻居节点健康报告，这些报告用于周期性地更新其邻居节点的状态。

为了让测试员能完全控制传输报文，网络层函数库还提供了一个重要的功能——基于位的报文修改。这个功能允许测试案例可以修改网络层报文中的任何字段，包括报文头部和命令的有效载荷。此外，网络层和 MAC 层之间的接口允许使我们指定哪些 MAC 层头部中的字段可以修改以及如何修改。在我们的实现里，MAC 层头部中的每一个字段在 bitmap 类型的变量 bitMapHdrsManipulated 中都有一个相应的位，例如位 0 对应着 MAC 层头部的字节 0。如果变量 bitMapHdrsManipulated 中的某一位被置为 1，那么 MAC 层头部中对应的字节将依据从网络层收到的接口报文中的信息来进行修改。

多设备测试着重于评估被测设备的网络层操作。为了支持这些测试，Wi-HTest 引入了另一个重要的模块叫做模拟网络。该模块与网络管理器合作，通过配置多个虚拟设备，能够为一个被测设备模拟出一个虚拟的 WirelessHART 网络。这样被测设备会认为自己是在一个真正的 WirelessHART 网络中与多个设备进行交互，从而测试各种网络层的功能。

3. Wi-HTest 测试引擎

Wi-HTest 上位机的核心是一个 Wi-HTest 引擎。这个引擎是在 CINT 环境中执行的一个 C++ 程序。CINT 是一个 C/C++ 解释器，它的目的是缩短在处理 C/C++ 脚本时的编译和链接时间。测试引擎的一个重要的组成部分是脚本库。该脚本库提供了一系列支持函数来帮助生成各种测试脚本。

测试引擎的主要功能是读取测试脚本并产生相应的无线命令，然后将命令发送给被测设备。这些命令会被传送给网络层，组装所需的网络层头部并被发送给 RF 接口。然后，测试引擎等待从被测设备发回的响应报文并验证其正确性。另一方面，测试引擎将为测试脚本定义的各种超时维护相应的定时器。如果超时发生时还没有从被测设备收到预期的响应报文，那么测试引擎将会报告相应的错误信息。

#### 11.2.2.3 RF 接口设计

为了能让 Wi-HTest 上位机和被测设备通过 WirelessHART 协议进行通信，我们

用 USB 电缆将 RF 接口连接到上位机上。RF 接口是 Wi-HTest 上位机和被测设备之间的桥梁。图 11-6 描述了 RF 接口的整体架构。

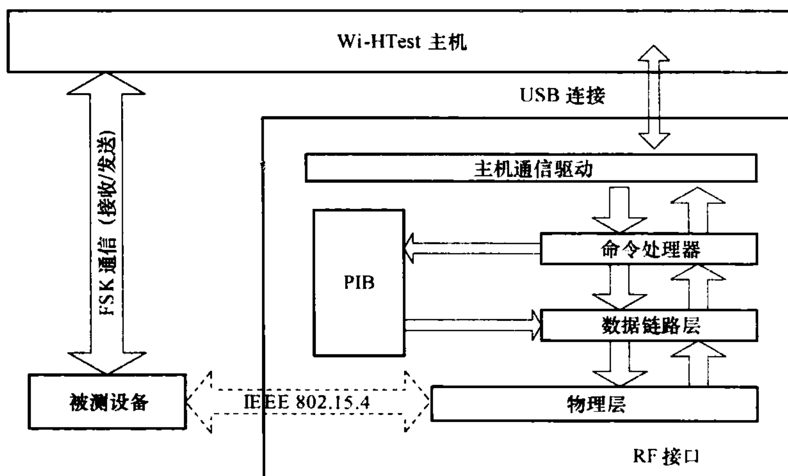



图 11-6 Wi-HTest RF 接口架构

1. 硬件平台

我们的 RF 接口是在 FreeScale Coldfire V1 工具包上实现的。这个硬件平台具有以下一些属性：

1）最高频率达 50.33MHz 的 ColdFire V1 处理器。

2）高达 128KB 的闪存和高达 16KB 的随机存储器，并带有硬件加密电路。

3）支持四种低功耗模式。

4）板载逻辑分析器和虚拟串行端口。

5）支持 USB 设备模式和 USB 上位机模式，并有 Mini-AB USB 接口。

6）8 个用户 LED 指示灯和 5 个按钮。

这个硬件平台足够满足 WirelessHART 标准所定义的严格的时序要求。

2. 实时嵌入式伪协议栈

RF 接口上的数据链路层和物理层被统称为 WirelessHART 伪协议栈，这是因为我们把网络层剥离开来并放置在 Wi-HTest 上位机上。这个伪协议栈是完全符合 WirelessHART 标准的，这也意味着它必须满足标准中定义的严格的时序要求。为了解决这个严格的时间同步问题，我们使用了以下几种解决办法：

①使用 AES-128 来加密一个数据帧和解密其相应的确认报文都可能会使得协议栈失去同步。为了加快加密/解密过程，我们采用了一种流策略。例如，当接收报文时，协议栈在收到第一个 16 字节数据时就开始进行解密。这样，计算量大的安全检查工作就能按时完成。②我们让中断处理程序尽可能简单。只有那些时间关

键的工作会放置到中断处理程序中，而非时间关键的工作将被推迟并在适当的时候才被处理。③我们给予 MAC 层最高的调度优先级。每当有数据帧要处理时，MAC 层可以抢占所有其他任务的 MCU 资源。有时候，MAC 层上可能有多个待处理的任务。对于这些任务，我们进一步给定不同的优先级来确保协议栈的时间同步。例如，传输一个数据帧比从指令处理器接收一个数据帧具有更高的优先级。

3. 命令处理器

RF 接口是 Wi-HTest 上位机的无线接入点，所有的测试命令都通过它来发送给被测设备，并且所有的测试响应数据都由 RF 接口来捕获并发送给 Wi-HTest 上位机。RF 接口的核心是一个指令处理器，所有的命令报文和对应的响应报文都由这个指令处理器来进行处理。

RF 接口和 Wi-HTest 上位机之间交互的报文有三种类型：

1）接口配置命令：上位机发布此类命令用来配置 RF 接口。

2）测试命令：上位机发布此类命令并通过 RF 接口发送给被测设备。

3）测试响应：被测设备返回给上位机的响应报文。

我们使用简单的通信协议来区分上述这些报文，并提供错误检测和重传机制。在初始化过程中，RF 接口等待从上位机发来的配置命令。RF 接口在被正确配置后，即可开始接收各种测试指令，也可接收从被测设备发回来的响应报文。如果是测试命令，RF 接口把它们封装在 WirelessHART 的 MAC 帧中，然后传递给数据链路层。数据链路层将进一步把报文发送给被测设备。在另一个方向上，RF 接口收到从被测设备发回的响应报文后，它会通过 USB 连接把这些响应报文返回给 Wi-HTest 上位机。

虽然 Wi-HTest 仅仅是一个测试工具，但是对于被测设备而言，它就如同加入了一个真正的 WirelessHART 网络并受其管理。从这个意义上说，在 Wi-HTest 工具中，网络管理器、网关和接入点是紧密结合在一起并协同工作的。不仅如此，Wi-HTest 还支持各种测试功能，比如故意加入一些故障信息。

为了通过 FCC 测试，Wi-HTest 工具还可以产生连续波。连续波是一个使用未经调制的传输测试模式。它也可以用来在某个信道上产生干扰。测试脚本可以发送命令 64529 到 RF 接口来启用或禁用此功能。

## 11.3　后期处理套件

Wi-Analys 工具捕获和记录所有无线报文，并形成日志文件。后期处理套件处理这些日志文件以检查所有的报文是否都符合标准。使用日志文件的好处有两个方面。首先，日志文件可以为最终的符合性检查提供原始数据；其次，当被测设备未能通过检测时，这些日志文件可以作为辩护证据。

后期处理套件判断符合性测试的成功与否。对于每个测试案例，一个后期处理程序读取日志文件，并对其进行分析。针对不同的测试案例，后期处理程序会检查被测设备发出的报文顺序、传输的时间点、报文之间的关系、报文内容等。如果这些全部符合标准，那么设备就通过了测试。否则，与标准不符的地方将被记录和报告。

Wi-Analys工具所产生的日志文件是纯文本文件。用户可以手工地检查Wi-HTest工具和被测设备之间交互的正确性。这样，设备在后期处理套件被完全开发完成之前，就可以完成认证。换句话说，当没有后期处理套件时，设备也能通过手工的方式来认证。

Wi-HTest工具、Wi-Analys工具和后期处理套件组成了完整的一致性检测环境。在这个检测环境中，被测设备一般要通过以下几个步骤来完成HCF认证。一个完整的测试由一系列的测试案例组成。在Wi-HTest工具运行每一个测试案例的同时，Wi-Analys工具会捕获在运行过程中的所有报文。尽管Wi-HTest工具可以决定一个被测设备是否通过了某些测试案例，但是后期处理程序将针对每一个案例分析其对应的日志文件，从而判断该设备是否在测试中严格地遵守了标准，特别是是否满足了严格的时序要求。被测设备只有通过了所有的测试案例，才能够得到HART基金会的认证。

# 第 12 章 HART 设备配备 WirelessHART 功能的快速方法

摘要：WirelessHART 标准是对传统 HART 标准的一种扩展，使其具备了无线功能。支持 WirelessHART 标准对于现有的 HART 设备而言是很重要的。WirelessHART 标准专门定义了一种 WirelessHART 适配器。利用这种适配器，有线 HART 设备就可以通过 WirelessHART 网络连接到上位机。在这一章中，我们遵照 WirelessHART 适配器的基本原理，提出一个为 HART 设备配备 WirelessHART 功能的快速方法。该方法不用对现有的 HART 设备改变太多。在完全集成的 WirelessHART 设备被开发出来之前，该方法可以作为一个过渡性的解决方案。在许多情况下，该方法可能也是 HART 设备供应商的最终解决方案。

## 12.1 WirelessHART 适配器

WirelessHART 标准定义了一种称为 WirelessHART 适配器的设备类型。WirelessHART 适配器不只是电缆的更换，而是一种具备 HART 功能的智能设备和强大的系统集成工具。WirelessHART 适配器可作为独立设备加入到 WirelessHART 网络中，同时也可作为主设备而与传统的有线 HART 网络相连。有线 HART 网络上的所有设备都可以通过 WirelessHART 适配器来与 WirelessHART 网络通信，也可以被上位机作为 WirelessHART 适配器的子设备而单独寻址。WirelessHART 适配器提供了一个成本高效的连接，从而将现有 HART 设备的智能化功能整合到控制和资产管理系统中。

## 12.2 简化版 WirelessHART 适配器

此外，我们建议把 WirelessHART 适配器作为元件连接到任何传统 HART 设备上，这样的适配器我们可以称之为简化版适配器（adapterlite）。简化版适配器附着到某个 HART 设备，这样他们看起来就像一个 WirelessHART 设备。HART 设备无需改变就可通过 HART 线缆连接到简化版适配器。在由简化版适配器和 HART 设备组成的有线 HART 网络中，简化版适配器作为主设备。而对于外界的有线 HART 或 WirelessHART 网络而言，简化版适配器对外呈现为一种 HART 设备。

一个简化版适配器是由以下几个部分组成的。

1）一个连接到 HART 设备的 FSK 端口。这用作主设备来控制 HART 设备。

2）一个 WirelessHART 协议栈和天线。这用来代表 WirelessHART 网络中新组成的 WirelessHART 设备。

3）另一个对外的 FSK 端口。这用于为新组成的 WirelessHART 设备提供对外的有线 HART 接口。

以下是简化版适配器的工作流程：启动后，简化版适配器将与 HART 设备通信并检索所需的设备信息，如设备 ID、标签等。然后，该简化版适配器将复制该 HART 设备的身份信息。最后，该简化版适配器等待着被初始化，这个初始化过程可以通过外部 FSK 端口或无线网络来完成。

简化版适配器将处理所有无线和有线 HART 命令。当处理一个命令时，简化版适配器根据是否必要而可能发送相应的命令响应给 HART 设备，或者使用不同的命令来检索任何信息。简化版适配器收到与其相连的有线 HART 设备发出的命令，也会将该命令转发出去，就好像该命令是发起于简化版适配器自身一样。如果有线设备支持 HART 第 7 版，那么简化版适配器承担的任务将会是最简单的。它可以在两个方向上转发大部分的命令，而不需要做太多的更改。

我们可以从头开始开发简化版适配器。或者，我们可以直接基于一个标准 WirelessHART 适配器来开发简化版适配器；如果采用基于标准 WirelessHART 适配器的方式，适配器的硬件部分不需要改变，而适配器的软件部分只需要一些简单的修改：

1）在 HART 网络上仅承认一个从设备。

2）接管从设备的身份标识，而不是将其作为子设备记录下来。

3）将 HART 设备当做自己的内部数据源器件一样的对待，而不是像上位机与子设备间的报文路由器一样直接响应上位机。

WirelessHART 适配器也能够处理早期版本的 HART 设备。因此，由适配器派生成的简化版适配器也可以自动处理早期版本的 HART 设备。采用简化版适配器的方式有以下两个重要特点：

1）不需要改变 HART 设备。只需要将简化版适配器附加到 HART 设备，我们就可以使该 HART 设备成为 WirelessHART 设备。

2）简化版适配器是万能的，因此它可以被附加到任何 HART 设备上。

一旦需要将有线 HART 设备开发成高度集成的 WirelessHART 设备，简化版适配器就可以成为解决方案的一部分。其具体实施方式是：去除内部 FSK 连接，将 HART 设备和简化版适配器的电路整合成一块电路，并将大部分软件（如堆栈）保留在简化版适配器中。

# 第 13 章 开发建议

摘要：相比基于 PC 的应用程序开发，嵌入式系统开发的难度要大得多。本章汇集了我们在 WirelssHART 协议栈开发过程中的一些经验，这些亲身经历的经验来源于 Wi-HTest 工具的自主研发过程。Wi-HTest 工具能提供 WirelessHART 设备所需的全部功能。我们还将介绍：WirelssHART 协议栈是否需要一个实时操作系统、怎样给接收到的报文打上时间戳、协议栈各层间的部分 API、支持时隙功能的定时器模块、硬件选取以及其他一些相关的问题。

## 13.1 嵌入式操作系统

PC 需要操作系统才能运行应用软件。操作系统为应用软件提供了运行环境，这样应用程序软件只需要实现其本身所具有的功能，如文字处理、画图等。因为需要支持应用软件的所有需求，所以通用操作系统对内存的要求通常比较大，从而可能导致应用软件的性能由于操作系统的原因而降低了。

一个嵌入式系统通常只有含有一个目的单一的应用软件，因而嵌入式系统中的操作系统也仅需为这一个应用软件服务。因此，嵌入式系统中的操作系统和应用软件在某种程度上可以被看成一个单一的软件块。因为嵌入式应用软件通常不需要操作系统提供的所有服务，并且嵌入式系统平台只有有限的内存空间和处理器速度，所以很多应用软件只包含操作系统的部分功能；此外，嵌入式系统对时间的要求迫使操作系统需要提供额外的实时性支持。嵌入式操作系统大多数都是实时操作系统(RTOS)，因此在某种嵌入式操作系统之上开发 WirelessHART 协议栈是合理可行的。

操作系统的一个作用是便于应用软件的开发。但是应用软件，尤其是嵌入式应用软件，可以不使用操作系统提供的任何服务。FreeScale 提供的 ZigBee 开发包就是一个典型的例子，这个源于 BeeKitTM 的项目不需要链接到任何操作系统库。该应用软件启动后，将进入无限循环；每次循环选择一个任务并且执行完毕。不在操作系统之上运行 WirelessHART 协议栈也有一些好处。首先，节约内存，减少运行时间；其次，WirelessHART 协议栈只需要较少的操作系统服务。但是，如果完全不用任何操作系统，那么开发 WirelessHART 协议栈的程序员需要有足够好的计算机科学背景，从而能开发某些软件来取代操作系统提供的服务。

## 13.2 对收到的报文盖上时间戳

WirelessHART 数据链路层使用了 TDMA 技术。为了保持良好的时间同步，对收到的报文打上精确的时间戳是一件至关重要的事情。然而，对于何时给报文打上时间戳，WirelessHART 标准的描述却有一些含糊。到底是在报文的前导码之前、前导码之后、分隔符之后，还是在物理层头部之后打上时间戳呢？这实际上是一个协议栈实现的问题。WirelessHART 标准只需要选取一个打时间戳的地方，然后整个 WirelessHART 系统自始至终都在同一个地方打时间戳。这样，任何 WirelessHART 协议实现都可以利用中断处理程序中获得的时间戳，来推导出报文中任一点的时间值，因为报文总是以恒定的 250KB/s 的速率到达。当然，对于不同的硬件平台，我们必须知道中断是由什么事件触发的，是由接收到前导码触发的？还是接收到报文长度触发的、或者是其他一些事件触发的？例如，FreeScale MC1320 射频模块就可以设定中断在多个时间点上触发，如当报文抵达时、当物理层头部得到报文长度时、当报文结束时、或者每当接收到 2 个字节时。MC1320 射频模块在这些时间点上都可以产生中断。我们可以在任何一个中断内计算出报文中任何字节的抵达时间，并加盖时间戳。至于如何获得时间戳的值，我们只需在中断处理程序开始时读取时钟值即可。MC1320 射频模块可以在其内部寄存器里保存时钟计数器的值。因此，采用 MC1320 射频模块得到时间戳的另一种实现方法是在下一个报文到达之前读取时钟计数器的值。

## 13.3 协议栈各层的实现

WirelessHART 协议栈的每一层都可以作为一个库或者一个任务来实现。如果采用库的形式，那么每一层就是一些 API 的集合。上层的 API 调用下层的 API，然后下层的 API 可能再调用下下层的 API。协议栈可以用一个任务来发送报文，用另外一个任务来接收报文。这种方式对于小规模的协议栈实现很有效。然而，WirelessHART 协议相比于其他类似的协议（如 ZigBee）来说要复杂得多，它是高端的低功率无线网状网络。我们推荐把每一层作为一个任务来实现，各层之间的通信通过各任务间的消息传递来实现。低层的任务由于时间限制紧，所以需要具有更高的优先级。这种使用任务的方式与 WirelessHART 定义的各层之间的接口也非常一致。

## 13.4 协议栈相邻层之间的 API

WirelessHART 标准定义了各层之间的 API，也就是服务原语（SP）。这对于描述各层之间的交互和什么信息在各层之间传送是很重要的。但是，这些是一个协议栈内部实现的问题，其他设备或者上位机并不知道其具体的实现。因此，为了满足特殊需要（比如想要传递额外的数据或者限制某些信息的传递），具体实现可以定义与 WirelessHART 标准不同的 API。实际上，WirelessHART 标准中定义的 API 只能作为一种参考。一些必需的细节信息在 WirelessHART 标准中并没有定义，例如：

1）WirelessHART 标准没有像 IEEE 802.15.4 标准一样明确定义个人区域网络信息库（PAN Information Base，PIB）的属性。某些属性，尤其是一些与入网过程相关的属性，可以在数据链路层或网络层中实现。还有一些属性必须可以被数据链路层和网络层访问。

2）入网过程本身需要网络层和数据链路层之间的紧密配合。实际上，“网络层规范”中的第 9.4.2 节描述了数据链路层在入网过程中承担的任务。

3）对于“数据链路层规范”中的 TRANSMIT.indicate 服务原语，虽然 WirelessHART 标准定义了 localStatus 参数的含义，但是并没有分配具体的位置。此外，一些实现可能需要加入 handle 这个参数。

4）“数据链路层规范”中的 RECEIVE.indicate（localStatus，packetRSL，payloadDLPDU）服务原语可以用于像抓包器这样的工具。为了实现这个原语，必须考虑到很多问题：什么时候设置射频模块为监听模式？怎么样不过滤掉带有任意目标地址的报文？上层怎么样解析数据链路层的 payloadDLPDU 参数？

5）“物理层规范”中的 API 没有说明怎样获得所接收报文的时间戳。如果只有规范中定义的那些物理层接口，那么数据链路层只能在 ENABLE.indicate（）或者 DATA.indicate（rsl，data）这两个原语开始的时候读取时钟作为时间戳，而这会由于网络延迟而不准确。一个实际的实现需要为 ENABLE.indicate（timestamp）或者 DATA.indicate（rsl，data，timestamp）原语定义 API，或者加入一个新的原语来读取最近一次收到的报文的时间戳。

## 13.5 定时器模块

在 WirelessHART 网络中，所有设备的通信时隙必须严格地为 10ms。从网络形成开始，时隙号就开始累加。所有的设备都必须时间同步，并且在每个时隙内的行为（空闲、发送或者接收）都被事先调度分配好。在每个发送或接收时隙内，设

备必须要在不同的时间点做出正确的动作，才能保证一次成功的通信和时间同步。由于一个时隙内两个时间点之间的时间很短，所以动作的执行任务很繁重，并且处理器由于能耗限制而功能有限。因此，传统的一次设置定时器的方式可能行不通。本节将描述我们在 Wi-Test 中是如何实现定时器模块的。我们创建了一个 standard-conscious 定时器模块，根据时隙类型自动产生一系列的时间中断（Song 等，2008 年）。此外，我们把动作划分为同步部分和异步部分，同步执行的动作在中断处理程序内完成。

### 13.5.1 WirelessHART 标准中的时隙

时隙内的时序请参考第 3 章中的图 3-4。在图 3-4 中，上图描述了发送方的时序，下图描述了接收方的时序。设备事先就被分配好了在每个时隙内的动作——空闲、发送报文或接收报文。

如果设备在某个时隙内被调度为发送报文状态，那么它首先等待 TxCCAOffset 段时间，然后马上开始执行 CCA，接着在报文发送完毕后开始在 TsRxAckDelay 时间段内监听接收方发出的确认报文。这个监听状态的持续时间为 TsAckWait。

如果设备在某个时隙内被调度为接收报文状态，那么它首先等待 TsRxOffset 段时间，然后开始监听报文；如果过了 TsRxWait 还没有监听到报文，那么它就停止监听。如果监听到了报文，那么它在报文接收完毕后的 TsTxAckDelay 时间内开始发送确认报文。

对于两个相互通信的设备，它们之间的通信时隙必须彼此同步，它们时隙内的时序也必须同步。这样才能保证在时钟漂移的情况下这两个设备仍能成功地通信。

### 13.5.2 基于 WirelessHART 标准的定时器模块

图 13-1 描述了定时器模块设计的组件。除了基于当前上层的执行动作来设置下一次的超时时间之外，定时器模块还需要知道 WirelessHART 标准的所有时间需求，并且占用很少的资源来管理这些时间需求以适应低性能的处理器。只有计算量大的任务才留给上层异步执行。

（1）硬件定时器　任何硬件平台都支持硬件定时器。硬件定时器可以按照设定的计数器值，在其到期之后就触发中断。对于 WirelessHART 标准而言，硬件定时器必须达到微秒级。

（2）WirelessHART 定时器模块　这是定时器设计的核心组件。WirelessHART 定时器模块以硬件定时器为基础。当某次超时引发中断时，WirelessHART 定时器模块首先检查自身状态以确定超时的语义，然后执行相应的代码（如果必要就给上层 MAC 层触发一个超时事件），再设置下一次的定时器超时时间。

如果本次超时表明是一个时隙的开始，定时器模块首先检查该时隙的类型；如

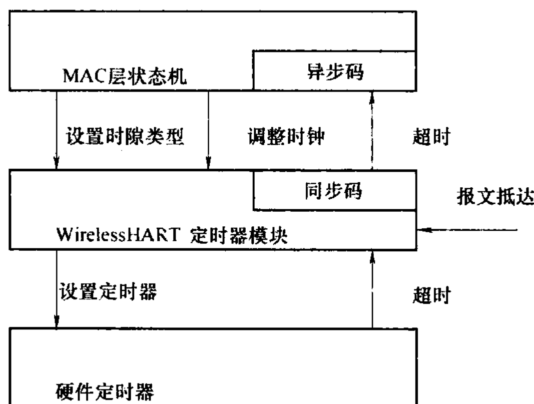



图 13-1 定时器模块设计的组件

果这个时隙类型是空闲时隙，那么定时器模块就会设置下一次的超时时间为 10ms 之后，即下一个时隙的开始。

如果这个时隙的类型是发送时隙，那么定时器模块首先向上层触发一个事件，然后设置下一次的超时时间为 TsCCAOffset。当设定的 TsCCAOffset 超时时，设备会开始执行 CCA 并且准备发送报文。然后，定时器模块会设置下一次的超时时间为 TxMaxPacket + TsRxAckDelay，用来让设备监听确认报文。如果没有报文需要发送，定时器模块将设置超时时间为下一个时隙的开始。如果接收方不需要对报文作出确认，那么下一次的超时时间将会在报文发送完毕后被设置为 TsRxAckDelay。当设定的 TsRxAckDelay 超时时，设备会将其射频电路设置为接收模式来监听确认报文，并且设置定时器模块的超时时间为 TsAckWait。当 TsAckWait 超时时，定时器模块将设置下一次的超时时间为下一个时隙的开始。如果设备没有收到确认报文，它会执行错误处理程序。如果设备在超时之前收到了确认报文，那么定时器模块就可以直接设置超时时间为下一个时隙的开始。

如果这个时隙的类型是接收时隙，那么定时器模块首先向上层触发一个事件，然后设置下一次的超时时间为 TsRxOffset。设备在等待 TsRxOffset 段时间后将开始监听报文，并且定时器模块设置下一次的超时时间为 TsRxWait。如果 TsRxWait 直到超时都没有报文到达，那么定时器模块将设置下一次超时时间为下一个时隙的开始；如果在 TsRxWait 期间有报文到达，那么定时器模块将设置超时时间为 TxMaxPacket + TsTxAckDelay。一旦设备能确定到达报文的长度，那么刚刚设定的超时值将被调整为报文结束后的 TsTxAckDelay。于是，当设定的超时时间达到时，设备将发送确认报文，并且定时器模块设置下一次的超时时间为下一个时隙的开始。

定时器模块也会在报文抵达时收到中断。设备利用此中断来记录时间戳，从而

实现设备间的时间同步。

(3) MAC 状态机　MAC 状态机是 MAC 层实现的一部分，其负责满足 WirelessHART 时隙的时间要求。由于大部分的工作都转移到定时器模块里面实现了，所以 MAC 层状态机只需要设置下一个时隙的状态、调整本地时钟以及执行定时器代码中的异步部分。

MAC 层状态机必须做的一个工作是事先告诉定时器模块未来时隙的类型，否则就会导致接下来的时隙类型被默认为空闲时隙。此外，定时器模块也需要在 MAC 层状态机的指导下调整时钟。这个时钟的调整与很多问题有关，包括接收报文的时间戳。定时器模块自身不能单独决定是否调整时钟以及如何调整时钟。

在任意两个连续的超时时间点之间，设备必须执行某些任务。其中一些任务必须被立即完成，另外一些也许可以推迟执行。我们把这些任务分为同步部分和异步部分。同步部分的任务在定时器模块里面实现，它在超时发生时的中断处理程序里被执行。同步部分的任务中有些任务是设置下一次超时时间、设置接收状态、开始传输报文以及执行一些不是特别紧急但是时间很短的任务。每当超时事件发生时，定时器模块会把超时类型发送给 MAC 状态机，并且向 MAC 状态机触发一些事件。然后，MAC 状态机能够异步地执行两个连续超时时间点内需要执行的剩余任务。其中一些任务也许在下一次超时到来时都还没有被执行完毕，例如解密、调用链路调度程序、准备确认报文等。如果某个任务执行完毕的时间太晚了，以至于设备在这个时隙内不能正常工作，那么错误处理程序将会被执行，当前时隙内的正常动作也许会被中止。但是，这不会影响两个交互设备之间的时间同步。

### 13.5.3 实现

定时器模块可以相当高效率地实现。下面是一段用 C + + 写的简单代码：

```
mCurrentTimeoutType = mTimeoutType[mCurrentSlotType][mTimeoutIndex];
  /* Set the next timeout */
  if(mTimeoutIndex = =0){ /*一个新时隙开始*/
    mASN + +;
    mASNTime = mCmpTime;
    mRxTime = mASNTime + mInterval_TsTxOffset;// 期望的接收时间
    mGetRxStart = FALSE;
    mCurrentSlotType = mNextSlotType;
    mNextSlotType = eMacTimerIdleSlot;
    mTimeoutIndex = mTimeoutsPerType[mCurrentSlotType] -1;
```

```
        mCmpTime = mASNTime + mTimeoutInterval[mCurrentSlotType][mTimeoutIn-
            dex];
    } else {
        mTimeoutIndex--;
        mCmpTime = mASNTime + mTimeoutInterval[mCurrentSlotType][mTimeoutIn-
            dex];
        if(mTimeoutIndex = =0) {
            if(mPositiveAdjust) {
                mCmpTime + = mAdjustTime;
            } else {
                mCmpTime - = mAdjustTime;
            }
            mAdjustTime =0;
        } else if((mTimeoutIndex = = 1) && (mCurrentSlotType = = eMacTimerRe-
            ceiveSlot)) {
            mCmpTime = mRxTime + mInterval_TsMaxPacket + mInterval_TsTxAckDe-
                lay;//确认报文的发送时间是基于发送方的时间
        }
    }
    TMR2InitCompareRegister(mCmpTime);
    /* notify Mac */
    mpMacTimerCallBackFunction(mCurrentTimeoutType);
```

在其他一些类似标准中，低性能的处理器不得不被用来满足严格的时序要求。上述方法同样适用于这些类似的标准。

即使某个设备的处理速度太慢而导致其不能在一个时隙内正常地完成相应工作，但是这个设备表现出来的外部行为可能显示出其同样满足 WirelessHART 标准。

同步和异步组件间的工作划分可能取决于处理器的性能。

## 13.6 硬件的选择

在所有低功率、低速率的无线网状网络中，WirelessHART 在内存使用和能量消耗方面是处于高端的。在第 8.6.1 节中我们已经知道，仅仅为了存储数据链路层和网络层定义的数据结构中最必不可少的部分，就需要超过 7KB 的 RAM。

一个完整的 WirelessHART 协议栈的代码大小，我们无法给出准确的数字。作为参考，我们这里给出 Wi-HTest 接入点的代码大小（见表 13-1）。Wi-HTest 接入

点是在 FreeScale JM 128 开发板上实现的。

表 13-1　Wi-HTest 接入点的代码大小

| 代码部件 | 代码大小（KB） |
| --- | --- |
| 协议栈 | 40 |
| RTOS | 7 |
| 系统函数库 | 11 |
| CDC-USB 驱动器 | 11 |
| 加密引擎 | 20 |
| 开机管理程式（Boot Loader） | 3 |

Wi-HTest 内含的协议栈代码包括物理层、数据链路层和一个精简的应用层。注意这里没有网络层。对于加密引擎，我们采用了软件方式的加密引擎。如果采用加速硬件加密，就不再需要 20KB 的存储空间。大部分 IEEE 802.15.4 的芯片都提供硬件加密。

如果加密和解密过程所占用的时间可以忽略，那么大部分嵌入式处理器对于运行 WirelessHART 协议栈来说都足够快了。Wi-HTest 接入点采用的是 FreeScale JM128 CodeFIre V1 处理器，该 32 位处理器的运行速度是 28MHz。由于 Wi-HTest 采用的是软件加密引擎，所以 Wi-HTest 必须边接收报文边解密报文，这样才能够满足对 Wi-HTest 的要求。

WirelessHART 标准的底层使用的是 IEEE 802.15.4 标准。这样，一个很大的好处是符合 IEEE 802.15.4 的商业射频芯片可以直接用于 WirelessHART 协议栈的开发，并且不用担心芯片的质量问题。此外，这些射频芯片的开发包里面通常自带有硬件加速引擎。

最常见的商业解决方案是把射频芯片和处理器集成在一起。这种集成方式可以是片上系统（System-on-chip，SOC），例如德州仪器公司的 CC2430™芯片；还可以是系统内组装（System-in-package，SIP），例如 FreeScale 公司的 MC1321 和 MC1322 芯片。由于这些处理器的性能和内存大小通常有限，所以我们在选择这些芯片时必须要小心谨慎。在 WirelessHART 标准发布之前，用当时市面上的商业集成芯片来运行一个完整的 WirelessHART 协议栈还是很困难的。

## 13.7　一些相关问题

以下是一些使用 Wi-HTest 和 Wi-Analys 工具的设想场景：

1）在设备研发的初级阶段，设备可能可以接收到通告报文并且能发送出入网请求报文，但是代理设备一直无法接收到设备发出的入网请求报文。

2）这时，我们可以让该设备来加入 Wi-HTest 工具。然后，我们可以通过 Wi-Analys 观察到设备发送入网请求报文的时间比正常时间早了 2ms；经过分析发现，造成这种情况的原因是由于设备的时间偏差太大了。经过对该设备的时间进行调整后，Wi-HTest 工具最终能在其 MAC 层确认收到了设备发出的入网请求报文。

3）但是，后来发现 Wi-HTest 工具并没有对设备发出的入网请求报文做出响应。经过分析发现，造成这种情况的原因是入网请求报文的格式错了。经修正后，Wi-HTest 工具能够正常地响应设备发出的入网请求报文了。

4）后来又发现设备在 MAC 层并没有回复 Wi-HTest 发出的响应报文。经过分析发现，造成这种情况的原因是：在设备发送入网请求报文之后，由于设备的超时时间的设置有问题，所以当 Wi-HTest 发出的响应报文到达的时候，设备的等待时间已经超时了。在调整设备的超时时间值后，设备就能够正常收到 Wi-HTest 发出的响应报文，并且能将其传递给自己的应用层。

5）至此，研发人员就可以开发和处理入网响应功能了。

1. 时间就是一切

无线收发器只是在发送时隙和接收时隙内才被打开。并且在这些时隙内，无线收发器也只是监听一小段时间；这样就可以节约电池能量，但是同时也增加了协议栈实现的困难。设备经常会在报文到达的时候而没处于侦听状态，从而导致自己无法接收到报文。然而，当我们调试设备使其能够正常接收报文时，常令人沮丧的是：正在开发的设备发送了一个正确的报文，但是接收方对此没有任何反应。当利用 Wi-Analys 来检查时，发现报文也没有任何错误，最后观察 Wi-Analys 记录下的时间戳才发现报文发送的时间戳不对。因此，时间在 WirelessHART 系统开发中是至关重要的。

2. 怎么样计算中间硬件设备的延迟

从调用报文发送函数来启动报文发送到报文真正地被发送出去之间有一段延迟。因此，我们需要比预定的时间早一点启动报文的发送以弥补该段延迟，从而确保报文的准时发出。这段延迟时间可以通过传输中断来计算。传输中断是在启动报文发送时触发的。传输中断开始的时间与报文真正被发送的时间之间的差值即为该段延迟时间。

我们也可以用 Wi-Analys 工具来计算接收延迟。接收延迟是指从报文到达的时间到报文被加上时间之间的时间间隔。在发送时隙中，从调用报文发送函数到收到确认报文并打上时间戳之间的时间间隔包含有以下三个部分：发送延迟、从发送报文到接收到确认报文之间的传输时间、接收延迟。假设我们已经计算出了发送延迟，然后通过 Wi-Analys 的日志可以计算出第二个部分的传输时间，最后就可以计算得到接收延迟。

3. 时钟偏移算法

时隙内的时间点是通过处理器自己的时钟来实现的。WirelessHART 的时间单位是 μs，但是处理器的时钟滴答时间也许不能完全精确地划分成 1μs。例如，我们开发 Wi-HTest 所使用的 JM 开发板时钟频率为 24MHz，那么它的时钟滴答频率为 24MHz/16 = 1.5MHz。因此，我们不得不用 1.5 个时钟滴答来代表 1μs 以触发 WirelessHART 的计数器。为了调整微小的时钟偏移，我们需要周期性地增加或降低 WirelessHART 计数器的值。我们所使用的算法是在每一个时隙开始的时候偶尔会对 WirelessHART 计数器的值加 1 或者减 1。该算法定义了长计数器和短计数器，并利用这两个计数器来决定在哪些时隙该对 WirelessHART 计数器加 1 或者减 1。长计数器和短计数器都是用来记录时隙数的。每当长计数器的值发生溢出时，长计数器和短计数器的值都应该复位并重新开始计数。每当短计数器的值发生溢出时，该算法就在当前时隙对 WirelessHART 计数器的值加 1 或者减 1。该算法简单、通用并且容易实现，同时还能避免因为调整时钟而被跳过的时钟中断所引发的潜在问题。

我们开发所使用的 JM128 DEMO 开发板都各有自己的板载晶振。这些板载晶振彼此间的差异比较大，各自的时钟漂移率也不同。因此，我们需要对这些板载晶振进行调谐，使它们彼此间能以非常精确的相同频率工作。最终的 Wi-HTest 产品都使用了一种非常精确的晶体振荡器，从而不再需要对每个 Wi-HTest 产品分别进行调谐了。

这个算法现在还可用于错误注入调试。Wi-HTest 工具中的晶振能够被故意设置成漂移快一些或者慢一些，从而测试被测设备与时钟源保持时间同步的能力。该测试脚本中的晶振可以被设置成长周期漂移、短周期漂移以及漂移的方向。

4. 其他几点问题

1）对于物理层以上的时钟或定时器，我们可以使用一个时隙作为时间单位。

2）当构建通告报文的时候，一定要确保加入链路的方向是设置正确的。对通告报文中加入链路状态的设定是针对入网设备而言的，而不是针对发送通告报文的设备而言的。例如，如果发送通告报文的设备在加入链路时将处于发送状态，那么该加入链路应该被设置成接收状态。反之，如果发送通告报文的设备在加入链路时将处于接收状态，那么该加入链路应该被设置成发送状态。

3）在调试时，如果不是调试跳频技术，可以只保留一个信道，其余的信道全部设置为黑名单。

4）对于两个邻居设备 A 和设备 B，如果只有设备 A 被配置为设备 B 的路由器，那么网络管理器在对设备 B 进行链路分配时，一定要确保设备 A 和设备 B 之间已经分配有链路了。否则，设备 A 无法转发网络管理器发送给设备 B 的链路配置信息。同样对于任何设备之间的连接而言，先配置接收方再配置发送方将更安全。

# 第 14 章　WirelessHART 网络部署的建议

摘要：世界上成千上万的 HART 现场设备都拥有着丰富的现场数字资源。然而，这些资源并没有被上位机充分利用起来。在许多情况下，这些现场设备中的数字资源并没有被连接到工厂的资源管理系统。这时，无线技术的使用提供了一种既廉价又高性价比的方式来获取这些现场设备里的数据和诊断信息。一个完整的 WirelessHART 解决方案应该提供这种桥接功能。WirelessHART 设备很容易安装。现场设备的丰富数据可以通过标准接口，高可靠性地路由至上位机。并且，WirelessHART 系统不需要其他特殊软件就能实现现场设备与上位机之间的无缝连接。同时，这样也提供了一个很好的机会，使得用户可以轻松、安全地测试和使用非实时监控应用中的无线技术。

## 14.1　WirelessHART 网络范围

为了安装 WirelessHART 设备，工厂的工程师应该考察当前支持 HART 的现场设备和控制回路，然后决定在什么地方采用无线连接能够在最小的风险下带来最大的效用。不同工厂的各过程设备间均有诸多不同，但是它们也都有一些共同特征，这使得我们可以在网络设计方面应用一些共同的经验。对于网络规模比较小的 WirelessHART 网络，太少的网络设备无法最大化地体现出这种新技术的优势。另一方面，规模太大的 WirelessHART 网络又会降低网络的性能。对于像煤矿或化学工厂等大型设施，单个流程处理单元应该构成一个 WirelessHART 网络；对于一些垂直排列的设施，如发电厂或者工厂，每单层应该构成一个 WirelessHART 自组织网络。一个好的工程实践经验是：给每一个工厂区域和/或每个操作单元都安装一个网关，正如现在的自动控制系统和 I/O 系统布局那样。

## 14.2　WirelessHART 网络设计

WirelessHART 网络的配置可以与有线 HART 网络相似。WirelessHART 网关是远程 I/O 系统，它将 WirelessHART 现场设备、WirelessHART 适配器连接到 DCS、PLC 系统以及其他工厂自动化系统。WirelessHART 接入点是 WirelessHART 网关的 I/O 模块，它将 WirelessHART 现场设备和 WirelessHART 网关连接起来。WirelessHART 网关可以连接有一个或多个 WirelessHART 接入点。WirelessHART 网络的

一端是网关和接入点，另一端是现场设备。WirelessHART 接入点可以在物理位置上与网关分开，但是通常来说应该部署在与它相连的现场设备附近。

HART 基金会提供了一个简单的参考公式用于计算 WirelessHART 接入点的载荷，即多少个现场设备可以直接或间接地连接到一个 WirelessHART 接入点：

$$设备数 = 设备的平均数据更新率(AUP) \times 25$$

例如，当设备的平均数据更新率为 1s 一次时，那么一个 WirelessHART 接入点可以接入 25 个设备。当设备的平均数据更新率为 10s 一次时，那么一个 WirelessHART 接入点就可以接入 250 个设备。

连接设备数量的标准与其他任何传统 I/O 类似，就是不要阻塞 I/O。当不确定能具体连接多少个设备时，我们可以多安装几个接入点。虽然额外接入点会导致一些额外的成本，但是这些额外的接入点能提供更多的网络冗余路径，也可以使得 WirelessHART 网络更可靠。

HART 基金会同时还提供了以下公式，用以估算 WirelessHART 网络平均占用带宽：

$$网络平均占用带宽 = 设备数 \times (0.0001\% + (0.02/AUP))$$

式中，0.0001% 表示一些额外开销（如网络健康状态报告所占用的带宽等）；0.02% 表示数据传输和其他网络流量占用的带宽。

例如，当 100 个设备的平均数据更新周期为 1s 时，那么这 100 个设备会占用 2.01% 的总带宽。当 1500 个设备的平均数据更新周期为 60s 时，那么这 1500 个设备会占用 0.65% 的总带宽。

以上是相对比较保守的估计，没有考虑网络区域的大小。对于覆盖范围比较大的网络而言，网络设备彼此相距比较远，这样多个网络设备可以在同一时隙同时使用同一个信道。由于无线电能量随距离衰减，一个区域的带宽占用率比总的带宽占用率少。利用这个公式，用户可以评估 WirelessHART 网络能否与其他 2.4GHz 网络在同一工厂区域内共存。

WirelessHART 系统的一个巨大优势是 WirelessHART 适配器。WirelessHART 适配器可以安装在从现场设备到 I/O 模块间电流回路附近的任何地方。WirelessHART 适配器不但使得现有 HART 设备具有无线能力，而且解放了设计者。这样，设计者不必将设备放置在具有更好接收效果的地方，而可以将设备放置在其应该被安装的物理位置上。假设一个压力传感器必须安装在一个钢制容器的中心线上，而这个地方仅仅处于地板上 1ft（1ft = 0.3048m）高。这时，如果我们使用 WirelessHART 设备，那么为了更好的接收效果，我们不得不将该压力传感器与 WirelessHART 设备远程相连，或者不得不将天线与 WirelessHART 设备远程相连。然而，如果采用 WirelessHART 适配器，我们只需要在这个地方安装一个有线 HART 设备，然后把这个有线 HART 设备远程连接到一个 WirelessHART 适配器即可，这是一种既简单

又低成本的解决方案。

## 14.3 WirelessHART 网络部署

由于无需有线电缆穿过电缆槽，所以 WirelessHART 网络的安装比传统的有线 HART 网络更简单、更低成本。只需要简单地确定设备应该安装在工厂的什么地方，然后安装该设备，最后再安装 WirelessHART 接入点和网关即可；偶尔也可以加入一些路由设备。设备加入网络后，只需要简单的配置下该设备，然后该设备就可以开始运行了。WirelessHART 网络的安装与传统有线 HART（4~20mA）系统的安装一样简单，它们使用相同的工具和技术。一旦 WirelessHART 网关、接入点和设备都安装好了，WirelessHART 网状网络就可以自动形成，并开始正常的数据通信。

WirelessHART 设备预配置的方式与有线 HART 设备一样，其关键的区别在于 WirelessHART 设备需要一个加入密钥和一个网络 ID。设备利用网络 ID 来决定利用哪个通告报文加入网络（因为在某个区域内可能有多个 WirelessHART 网络）。一旦设备侦听到一个或多个邻居设备，那么该设备就可以向网络管理器发送一个通过加入密钥加密的入网请求报文。网络管理器对该设备进行认证，然后允许该设备加入到网络中。

WirelessHART 的自组织特性得到过程工业界的青睐，其部分原因是因为 WirelessHART 网络易于规划、定制和安装。与其他过程工业无线解决方案（如点对点网络）不同的是，自组织网络不需要详细的位置勘测和专用设备就能被部署。同时，自组织网络也更容易扩展。事先规划并且利用一些实际经验，也是成功运行的关键。

对于小型 WirelessHART 网络来说，网关应该安装在网络的中心。对于大型 WirelessHART 网络和应用而言，网关通常需要被安装在控制室或机柜房，与接入点相距较远；对于这种情况，最好的实践经验是先在接入点附近构建一个网络，然后扩展该网络直至达到遥远的过程单元区域。这种实践经验是建立更大型 WirelessHART 网络的基础。

网关为网络设备与上位机和控制室之间提供连接。网关负责接收响应报文，并且缓存和维护网络设备发出的响应报文。这些缓存报文的内容有突发模式的命令、事件通知报文和用于正常通信的 HART 命令等。这些缓存的响应报文是作为上位机应用请求的响应被返还的。网关还具有一些内置的额外功能用来支持适配器，使其能够透明地访问与 WirelessHART 适配器相连的现场设备。

大多数情况下，网关通过多个接入点与 WirelessHART 网络相连。当 WirelessHART 网络使用多个接入点时，网络管理器会将通信量调度分配给所有的接入点。如果某个接入点失效了，网络管理器将会自动调整资源分配，将网络通信量分摊给剩余的接入点。

Rosemount 公司的无线网关（Rosemount 1420）是一个 WirelessHART 网关的实例（见图 14-1）。Rosemount 1420 包含了网络管理器和安全管理器。Rosemount 1420 通过一个 Web 浏览器给用户提供界面，使得用户能够方便地对无线网络进行安全设置、运行诊断和配置信息。它同时也是后台上位机和 DCS 访问无线设备数据的入口点。Rosemount 1420 还能通过以太网或串口连接到支持 Modbus、OPC 和 TCP/IP 的设备或系统。

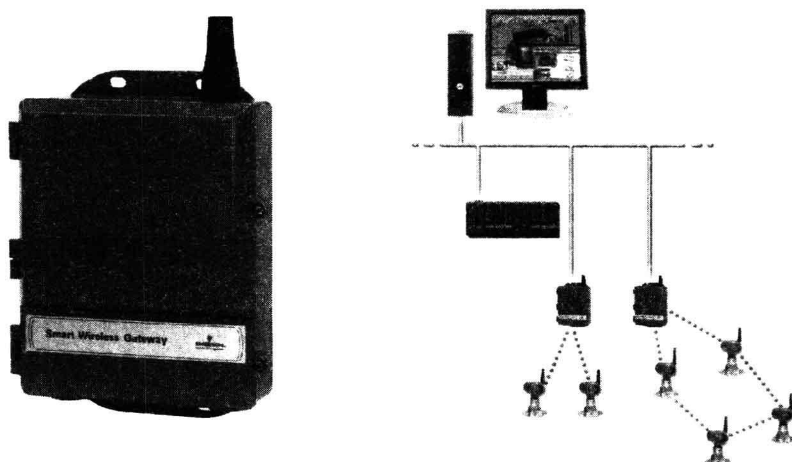



图 14-1 WirelessHART 网关的实例

大多数情况下，网关通过本地接口与控制系统相连，并显示为整个配置系统的一部分（见图 14-2）。在一些其他情况时，网关可以使用类似于 Modbus 和 OPC 等工业标准机制来实现与控制系统的互连。

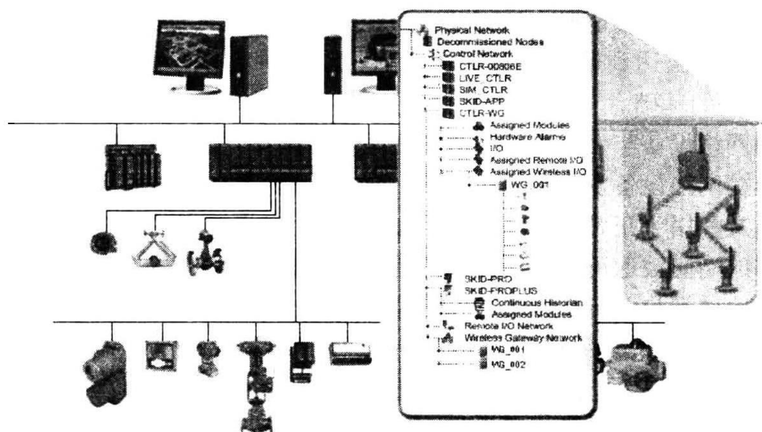



图 14-2 WirelessHART 网关与 DCS 的集成

## 14.4 更多建议

当考虑安装 WirelessHART 网络时，以下的一些建议也是非常重要的：

1）出于安全考虑，在 WirelessHART 网络中，设备信息必须要预先配置给网络管理器。这些信息将在设备加入网络过程中被用于检查安全和认证。加入密钥对于解密加入网络请求报文的载荷是必不可少的。为了安全，每个设备应该有不同的加入密钥。这样，网络管理器也必须存储有网络设备的设备 ID 和设备长标签。加入网络请求报文中也包含有网络设备的设备 ID 和设备长标签。所有 HART 设备的设备 ID 都是唯一的。然而，当我们替换一个失效设备时，利用设备 ID 来验证设备的方式会给网络管理器带来一些额外的工作。

2）当网络管理器为两个设备之间配置单播链路时，在接收链路被配置给接收方之前，发送方不要发送任何报文。

3）设备 ID 可以和入网密钥、网络 ID 一起预先记录在网络管理器中。将指定的设备安装在指定的位置，这样做更安全，但是这也许会导致设备安装和替换时出现一些问题。例如，工程师怎么知道一个设备应该安装在哪个位置？因此，真正关键的是将类型正确的设备安装在正确的位置。设备的标签可能标识有设备的物理位置。我们可以让网络管理器在设备加入网络之前记录下设备的标签，这样网络管理器就能够知道设备的物理位置。为了协助设备的安装，手持设备必须能够向现场设备配置入网密钥。

4）WirelessHART 网络要求设备拥有高度精准的时钟以保持时间同步。然而，并不是所有的设备在这方面都能达到要求。因此，网络管理器对于这些设备应该设置较短的 keep-alive 时间间隔。

5）成对的部署接入点可以提供更好的冗余，具体原因在第 9.6.2 节已经讲述。

6）虽然 WirelessHART 网络的部署不需要现场勘测，但是现场勘测是有益无害的。例如，我们可以通过现场勘测找到最适合安装路由设备的位置，这样可以获得最强的信号强度和最少的路由设备。

7）如果没有新设备想要加入网络，那么现场设备可以停止发送通告报文。这样可以避免绝对时隙数和其他网络信息暴露给有敌意的抓包器。

8）每个设备都有其自己的加入网络链路。两个相邻设备的加入网络链路可以在不同的物理频段上共享同一个时隙。网络管理器在配置链路的时候应该避免这种情况的发生，因为在这种情况时新设备将不知道该选择谁的加入网络链路。

# 第四部分　WirelessHART 展望

这一部分重点关注 WirelesHART 标准在过程工业无线中的地位。

第 15 章解释了什么过程工业采用 WirelessHART 标准、为什么 WirelessHART 标准已经准备好了、为什么 WirelessHART 标准成功的几率更大。

第 16 章讨论将无线技术应用到实时过程控制中的挑战。本章介绍作者如何利用无线通信技术来实现典型的 PID 控制。

第 17 章阐述无线技术应用到过程工业而引起的一些研究机会。

第 18 章展望无线和 WirelessHART 标准的未来，其中包括应用、产品和标准化。

# 第 15 章　过程工业采用 WirelessHART

摘要：过程工业现场对无线系统有应用需求，而 WirelessHART 标准很好地满足了这个需求。本书的整个第四部分都将讨论这个需求。在本章中，我们将展示为什么 WirelessHART 网络是理想的用于连接现场设备的无线方式。WirelessHART 标准是基于已经过验证的解决方案之上，包含了最先进的技术，并且易于采用。

## 15.1　WirelessHART 标准是基于已经过验证的解决方案之上

WirelessHART 标准发布于 2007 年 9 月，它是建立于多年严谨的前沿性实验基础之上的。在 WirelessHART 标准委员会成员开始起草标准的几年前，无线网络实际上已经被尝试应用到过程工业中。正是这些实验的成功促成了 WirelessHART 标准的诞生。所有这些实验的经验和教训都被纳入到 WirelessHART 标准中了。例如，以下就是这些实验过程中的一些重要发现。

1）功耗是一个非常关键的性能参数。用户期望任何现场设备在需要维护之前都能运行几年的时间。这就要求容量足够大的电池以及对能耗的智能化管理。

2）如果工业无线系统没有很高的可靠性，工业过程是不会考虑采用无线系统的。可靠性已经被谈论得足够多了。基本上，无线系统必须得像有线系统一样可靠，才能够引起足够的关注。

3）随着时间的推移，无线网络中的设备数量将会逐渐增多。无线技术不仅可以用于取代有线，而且还可以释放出一系列潜在的新应用。不远的将来将会出现拥有大量无线设备的无线网络。

4）客户将要求更快的更新率。任何无线解决方案必须在其设计中保证这一要求，以使其产品具有持久的生存期。

5）点对点通信是在工厂车间环境中是不可靠的。在工厂车间里，布置设备以使设备间能始终保持视距通信是非常困难的。最好的无线通信系统不得不通过网状拓扑结构构成，因为网状拓扑结构能提供多路径冗余。

6）任何无线网络必须能生存于拥挤和嘈杂的环境中。WirelessHART 就是基于这一假设的。

7）现场勘测是昂贵的，而且其成功的机会有限。由于工厂车间的动态变化，依据现场勘测而部署的设备可能很容易就失去彼此间的联系。

8）在网络规模比较大的时候，基于 CSMA 的冲突避免机制效果就不好。基于

这一发现，WirelessHART 标准用 TDMA 机制取代了 IEEE 802.15.4 标准中的 CSMA 机制。

用户的试验告诉了我们许多事情：在动态变化的现实工业世界中什么能有效工作、什么不能有效工作、什么是重要的、什么是不重要的。

## 15.2 WirelessHART 标准包含了最先进的技术

WirelessHART 标准是一种向后兼容、成本效益高的标准。工业领域要求一种简单、可靠、安全的无线通信技术。WirelessHART 标准利用一些常见方法使其满足了这样的要求。WirelessHART 标准同时也是 HART 标准，它能用于所有过程现场设备相关的应用，其中包括厂房及设备管理，报警和事件记录。这些应用还包括液位监测、流量监测、压力监测、温度监测、振动监测、气体检测等。在适当的时候，WirelessHART 标准也可以应用于闭环控制。WirelessHART 解决方案还得到了许多过程自动化供应商的支持。从过程控制的角度看，WirelessHART 标准提供了灵活性、可扩展性和互操作性。从无线技术的角度看，WirelessHART 标准包括了低功耗、低数据率网络中一些最好的无线技术。WirelessHART 网络是一种自组织网状网络，其关注于现场设备的通信。以下是 WirelessHART 网络的一些亮点。

（1）网状拓扑结构　最简单的网络拓扑结构是星形网络。树形网络拓扑结构更加灵活，但是实现起来更困难。最后一种网络拓扑结构是网状。网状网络很复杂，但是很健壮。WirelessHART 网络是一种灵活的、自组织的网状网络组织。WirelessHART 网络中的现场设备之间没有层次结构，所有设备都具备相同的网络功能。换句话说，WirelessHART 网络没有使问题复杂化的精简功能设备（Reduced Function Device，RFD）或全功能设备（Full Function Device，FFD）。每个发起和汇集报文的设备都是路由器。WirelessHART 标准能适应不同的应用和环境，也没有特殊的工程或安装要求，它可以覆盖一个很大的地理区域。

（2）安全　WirelessHART 标准在数据链路层和网络层同时使用了行业标准的 AES-128 加密算法和密钥，也提供了认证和加密功能。

（3）可靠性　由于 WirelessHART 网络采用了网状拓扑结构，所以它在网关和现场设备之间提供了多条冗余路径。报文路由可以绕过干扰和障碍物。WirelessHART 网络可配置成至少能容忍单点故障。由于网状网络的特性，WirelessHART 网络中的设备越多，WirelessHART 网络的可靠性就越高。

WirelessHART 网络还采用了其他技术来保证通信的可靠性：跳频；默认情况下启用的空闲信道评估；可设置的传输功率、其默认值为 10dBm；信道黑名单；确保满足监测和控制应用需求的优先级机制。

所有这些技术也有助于可靠的共存。WirelessHART 网络能容忍一定程度的干

扰，也是不容易被破坏的，还能最大限度地减少对其他网络的干扰。

（4）动态带宽分配　WirelessHART 标准节省地使用通信以延长电池的使用寿命。设备可以要求固定的带宽来发布过程和控制数据，也可以要求暂时的额外带宽来传输大量数据（例如传输振动谱）。当维修现场设备的时候，我们还可能需要加大或减少带宽的使用。

（5）自组织和自修复　在 WirelessHART 网络中，所有设备都向网络管理器提供一些统计信息，这些统计信息包括无线通信的信号强度、与邻居设备通信的可靠性、检测到的新邻居设备等。网络管理器梳理连接和路由，为了可靠性而改变连接和路由，增加内部连接使网络更具弹性，对网络通信量进行均衡以获得更快的速度和更低的功耗。如果 WirelessHART 网状网络中引入了某个障碍物，那么设备将会自动地找到最佳的替代通信路径；然后，原来的通信路径将会被重新调整。这样，信息就能继续被传送。所有这些过程都是由网络管理器自行处理的。现场设备中的应用程序完全没有意识到网络管理器的存在，而是连续不断地通过网关与所有的现场设备通信。

## 15.3 WirelessHART 标准易于接受

最新无线技术（如上一节讨论过的网状拓扑结构、自组织、自修复特性）的使用使得 WirelessHART 网络的应用变得很容易。HART 标准是基于许多引导性实验和用户需求的，所以这也使得其很容易被用户接受。此外，WirelessHART 设备的优点还在于它仍然是一种 HART 设备。

WirelessHART 标准工作组从一开始就树立了“简便”的理念——简便的配置、安装、支持和维护。

从设备的安装数量来衡量，HART 标准是最流行的过程工业通信协议。截止到 2008 年中，工业现场已经安装了大约 3000 万台 HART 功能的设备。任何围绕 HART 标准建立的技术都能快速地被采用并使客户受益。

WirelessHART 标准是 HART 标准的一部分，它利用了大量 HART 现有的技术、基础设施和实践经验。WirelessHART 标准的整个应用层依然遵循 HART 标准。利用 HART 命令结构，WirelessHART 设备能兼容 HART 功能的控制系统和 DDL。现有 DD 功能的应用程序或工具能像访问普通 HART 设备一样访问 WirelessHART 设备。WirelessHART 网络能做任何有线 HART 网络能做的事情，并且还能够做得更多。这使得其能将无线和有线设备透明地整合到工业控制系统中。用户可以将无线技术添加到现有已安装的设备或全新的设备中。因为 HART 标准支持各种各样用于测量和控制的现场设备和系统，所以 WirelessHART 标准也能支持各种各样用于测量和控制的现场设备和系统。

虽然工业无线技术看起来像是一个跳跃式的发展，但是 WirelessHART 标准实际上是基于 HART 标准的一个平稳的演进。事实上，利用 WirelessHART 适配器，传统的 HART 设备可以通过 WirelessHART 网络与传统的 HART 应用进程通信。

通过保持了相同的 HART 用户体验，我们可以节省很多前期培训费用。WirelessHART 技术允许其从现有已安装的 HART 系统升级演变而成，而不是为了一个全新的标准而重新构建基础设施。数以百万计的 HART 现场设备已经被安装在工业现场，这个事实使得升级演变的方式更具有吸引力。为了采取 WirelessHART 技术，客户可以先低成本地尝试使用 WirelessHART 系统，在了解它之后可以逐步地扩大应用规模，并最终全部采取 WirelessHART 技术。客户熟悉的用于配置有线 HART 设备的工具同样能够用来配置 WirelessHART 设备。

据估计，在现已安装的有线 HART 设备中，大约只有 25% 的设备进行了数字连接，这样用户可以充分利用数字信号携带的诊断信息。WirelessHART 标准提供了一种快速、成本高效的手段，用于将现场设备和其他资产连接到工厂车间网络。在不需要改变已安装设备的情况下，我们就可以给已安装的 HART 设备添加无线功能；然后，这些具备无线功能的 HART 设备将形成一个 WirelessHART 网状网络；最后，所有的诊断信息能够通过该 WirelessHART 网状网络传输给上位机，以供其使用。与此同时，有线 HART 设备中的过程数据仍然通过 4 ~ 20mA 电缆传输。

当安装一个全新系统时，我们可以去除系统中的 4 ~ 20mA 线，使 HART 设备彻底的无线化。这类 WirelessHART 设备的供电方式可以是电池、太阳能、工业过程产生的电源、环境电源等。于是，过程数据将通过无线网络数字化的传输。即使工业现场发生了这样的变化，中央控制室的上位机应用进程仍然可以是传统的 HART 模式。HART 标准比其他现场总线安装量多的一个重要原因是其安装简便。WirelessHART 系统的安装就更简便了。在安装了 WirelessHART 网关和接入点以后，WirelessHART 设备甚至不需要部署 4 ~ 20mA 电缆就可以自动地入网。

由于具备了将新旧设备融合在一起的能力，HART 标准使得客户可以在任何需要和期望的地方添加无线设备。

WirelessHART 标准采用了 IEEE 802.15.4 标准，这同时也降低了开发成本。IEEE 802.15.4 标准的芯片制造商已经有很多。这些芯片也可被用于开发相对简单、低成本的 WirelessHART 解决方案。WirelessHART 标准使用的是全球通用的 2.4 GHz 频率，这也意味着 WirelessHART 系统可以被部署在世界各地。

# 第16章　无线与实时工业过程控制

摘要：过程工业现场运行着各种不同的应用，从辅助型到关键型。它们可以被分为以下三类：C类为监测应用、B类为控制应用、A类为安全应用。作为一种新技术，无线技术被认为应先应用于监测，而不是先应用于控制。早期的无线设备应该为传感器，而不是执行器。大多数在设备级的无线网络应用是遥感记录和监测。虽然无线技术正被用于控制应用，但是无线技术在控制应用和安全系统中的广泛普及还需要很长的时间。虽然无线技术需要提前解决工业实时性的要求，但是传统的过程控制应用也值得再次关注。在这一章中，我们将从整体上讨论无线应用于过程控制的挑战，以及我们在无线技术用于闭环控制的初步研究。

## 16.1　无线控制的挑战

无线技术的研究和发展引发了人们极大的兴趣。无线技术用于控制工业不是一个新话题。许多工业组织（WINA™，ZigBee和ISA™）多年来一直在推动无线技术在控制工业的应用。为了将无线技术用于控制工业，我们不得不克服一系列众所周知的、已形成共识的挑战，如安全性、鲁棒性、延迟和功耗。在对那些关心的问题进行简略接触后，我们将分析基于传感器网络的控制问题。虽然传感器网络用于过程监控已经得到了广泛的研究（Akyildiz等，2002；Callaway等，2003；Caro，2004；Chen等，2004；Culler等，2004；Elbatt等，2006；Krishnamurthy等，2005；Nixon等，2004；Nixon等，2005；Sheldon等，2005；Soldati等，2008；Song等，2007；Vieira等，2003；Zhang等，2009），但是在控制应用中运用无线技术还处于初期的测试阶段（Chen等，2005；Hieb，2003）。虽然人们同意这最终将会发生，但是来自学术界和工业界的长期不懈的合作努力是必需的。这里列出了几个可合作的领域。

### 16.1.1　过程控制网络和无线控制网络

如图16-1所示，一个典型的过程控制系统有三个层次的网络（Blevins等，2002）。图16-2描绘了与图16-1对应的无线系统，即无线控制系统。图16-1的底部是实际管理工厂流程的控制网络。控制器通过控制网络与包括传感器和执行器在内的现场设备相连。控制器从传感器读取数据，并将数据写入到执行器中。网络协议通常是能提供实时性、并具有可预测性和高可靠性的工业标准。控制网络的数据传送范围小，并且控制网络的报文比较小。在这个层次的无线网络通常被称为传感

器网络。在第 16.1.2 节，我们将阐述其面临的挑战。

我们称中间层次的网络为区域控制网络。区域控制网络连接着控制器和工作站。控制器控制着工业现场中的设备，而工作站与用户进行交互。区域控制网络传送用于配置、控制命令、监测和诊断的用户交互数据。它对实时性要求较低，但仍需要良好的可靠性。区域控制网络的数据传送范围较大，并且其报文比传感器网络的报文更大。区域控制网络可以是一种利用通信行业标准或使用工业标准（如以太网）的专有协议。由于区域控制网络不直接与现场设备相连，所以我们可以使用商用无线网络来代替它。这个层次的无线网络所面临的挑战与商用无线网络面临的挑战大部分相同。

顶层网络是企业办公网络。企业办公网络通常通过一个或多个防火墙与控制系统相连。企业办公网络提供连接到一些企业系统，如会计、库存、管理决策系统等。企业办公网络对应的无线环境是商用无线网络。这个层次的无线网络没有流程控制相关的特殊挑战。当然，把控制网络连接到办公网络将带来一些安全问题。无线应用所面临的挑战是有据可查，过程控制中无线应用所面临的挑战也得到了广泛的研究。对于过程控制，一些无线相关的问题（如安全性、健壮性和电源）就变得更重要了。

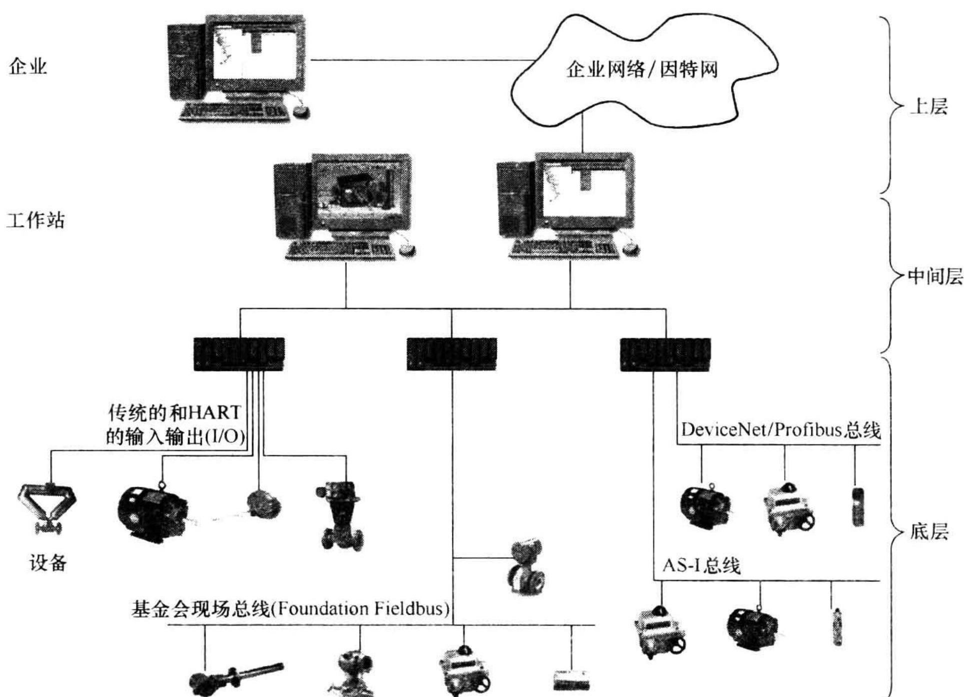



图 16-1　流程控制系统

由于社会原因，安全变得越来越重要了。将控制系统连接到 Web 加剧了安全方面的担忧。一些研究结果表明（Weiss，2005）：“控制系统容易受到攻击，因为它们没有被设计成满足 cyber 威胁；以及电子手段影响了控制系统的可靠运行，现实世界发生了 60 个以上这样的案例（虽然相关记录不公开）”。

无线安全是 2005 年 ISA 世博会期间最热门的话题之一。ISA 下属的 SP99 委员会定义了一套通用的控制系统信息安全需求。用户和厂商都可以参考该需求文档。

鲁棒性包括了可靠性和安全性。由于干扰和通信失败在过程工业现场变得更严重，因此鲁棒性也是一个值得关注的问题。在工厂的很多环境中，鲁棒性需要更加强大的天线。但是更高的传输功率会给易燃的环境带来危险并且造成更大范围的干扰。另一方面，在工业现场更换电池也是比较困难的。

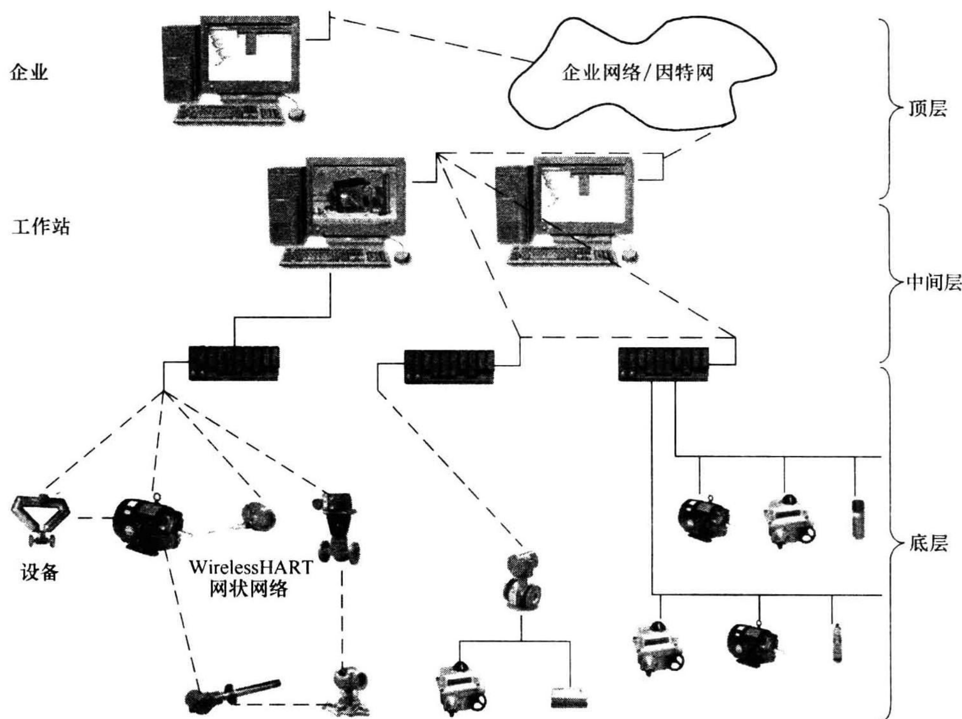



图 16-2 无线流程控制系统

## 16.1.2 基于传感器网络的过程控制

传感器网络相关的研究通常关注于对目标系统的监测。对于现有的工业控制系统，现场无线系统大多数扮演着辅助的角色，它们用于收集控制系统不能提供的一些额外数据。术语“传感器网络”无意识地将其范围限制在“传感”的范畴之内。

为了实现控制，我们还需要执行器，以及由传感器和执行器组成的网络。将传感器网络用于过程控制带来了一些技术挑战。无线技术的早期使用者目前正在测试基于无线技术的控制应用。

在闭环控制中使用无线通信来传送测量值还存在着很多挑战。为了最大限度地减少控制变化，典型的经验法则是：反馈控制的执行速度应该比过程响应时间（过程时间常量加上死区时间）快 4 ~ 10 倍。由于测量系统往往与控制系统不同步，所以测量值的采样速度通常远远快于过程响应时间（见图 16-3），在很多情况下，多回路控制器的采样速度比所需要的采样速度快 2 ~ 10 倍。

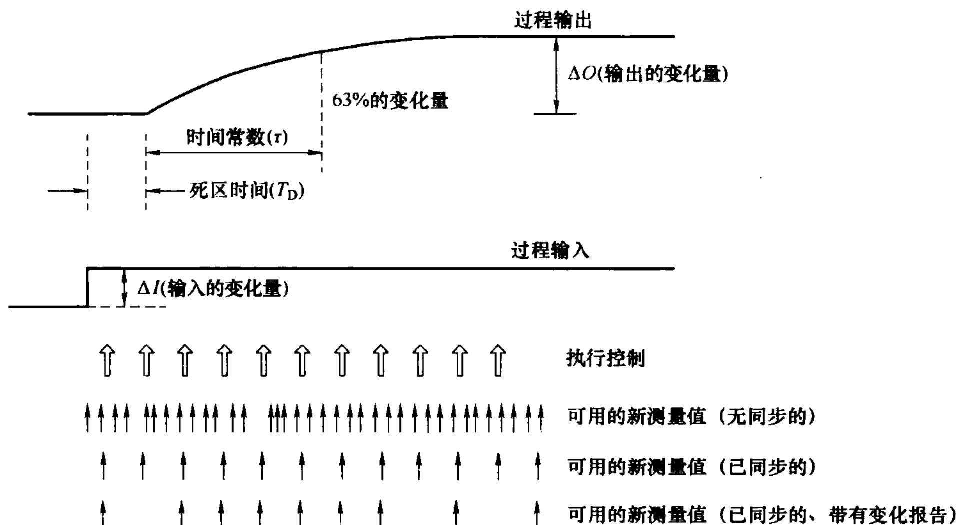



图 16-3　控制数据采样率

为了减少发送器的能量消耗，我们需要最大限度地降低测量值的采样频率。如图 16-3 所示，通过对测量和控制执行的同步，我们可以消除一些不必要的测量采样和通信。

在过程工业工厂中使用无线技术来替代有线技术会带来巨大的好处。用户一直希望能把无线技术应用到工业控制中去。对将来的无线技术而言，达到和当前现场总线相同级别的功能并不困难。我们相信如果工业界和学术界能够共同努力解决无线控制问题，这一天会很快地到来。

图 16-4 展示了一个大型流程控制系统中的传感器网络。图 16-5 展示了一个小型流程控制系统中的传感器网络。让我们来看一下它们所取代的现场总线。为了实现过程控制，现场总线网络通信及相关的控制功能和调度被设计成具有完全的确定性，并且控制系统中不能有通信干扰以及控制组织的变化。当前在网络能耗和通信优化上的工作将致力于为企业寻找最佳的调度算法。

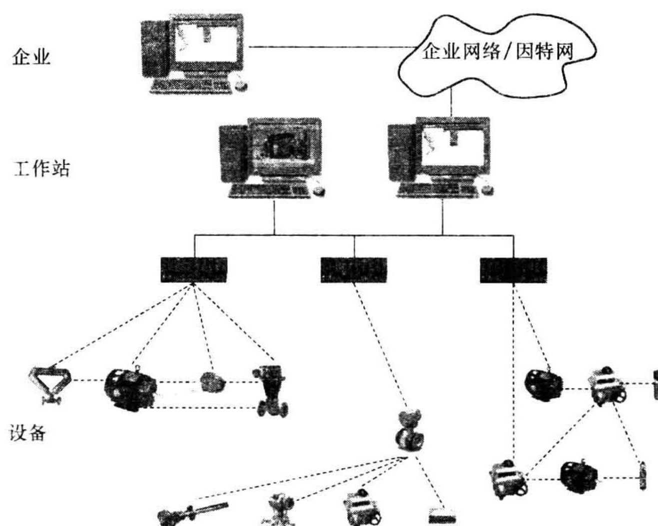



图 16-4 流程控制系统中的传感器网络（大型）

图 16-4 所示为传感器网络在大型流程控制系统中的一种可能实例。图 16-5 所示为传感器网络在小型流程控制系统中的一种可能实例。让我们来看看它们所取代的现场总线。为了实现过程控制，现场总线网络通信及相关的控制功能和调度都要被设计成具有很好的确定性。控制系统中不能有通信干扰或变化。针对网络能耗和通信的优化需要持续进行一段时间，以便寻找出最佳的调度算法。

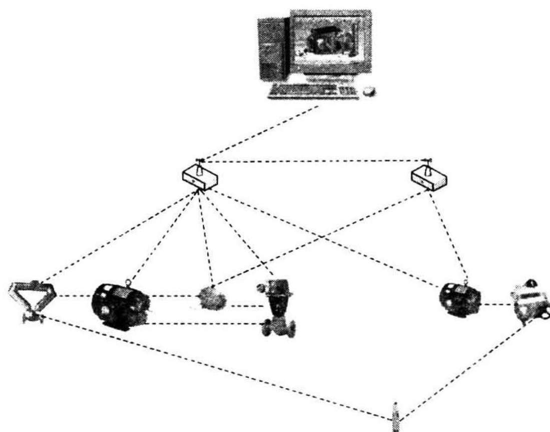


图 16-5 流程控制系统中的传感器网络（小型）

**（1）临时的干扰** 传感器网络使用空气作为通信介质。天空中无论发生什么都有可能会干扰数据传输。一些事件，如天气、移动的人或物体、其他无线信号，

都可能会干扰数据的无线传输。临时的干扰影响了数据的及时传输，这直接挑战了实时过程控制的目标。

（2）恒定的干扰　一旦现场总线被部署了，那么该现场总线将在控制系统的生命周期内一直工作。然而，无线控制网络在被部署了之后，其生命周期内还必须能被重新配置。由于增加或移除一些与无线网络无关的现场设备，两个节点间的通信可能会发生永久性的变化。

（3）电源的使用　直接与实时控制相关的电源问题包括断电的应急处理、电池水平引起的数据传输延迟的变化等。

除了现场总线可以完成的工作外，传感器网络还开辟了一些可能的新应用，以及这些新应用对实时控制带来的新挑战。下步措施之一是将传感器网络直接连接到工作站，而不是连接到专用控制器。小型系统中可能没有控制器，设备可以与运行有用户应用程序的工作站直接通信。将来，每个操作系统都应该具备实时操作系统的一些特性。如图 16-4 所示，大型系统仍然需要控制器，用于协调控制、数据处理和服务（例如，报警管理和历史数据收集）。

现场总线和传感器网络在许多方面存在着一些不同。虽然传感器网络本质上是不太可靠的，但是它利用多径技术进行了补偿。与现有现场总线网络相比，传感器网络的成本更低、传输速率更高，这也就意味着传感器网络允许部署更多的设备、允许监测和控制更多的过程数据。为了简单地模仿现场总线，传感器网络必须同步所有节点以便用全局时钟给数据打上时间戳，一个中央节点必须协调所有的数据流。这样必然增加了传感器的复杂性，而这又与传感器网络的其他目标相违背：降低成本、减少能量消耗、并有大量的小型传感器/执行器。

一个更好的问题可能会被问到：与现场总线相比，传感器网络如何能获得相等甚至更好的过程控制效果？传感器网络的实现方法是否与现场总线不同？在回答这些问题之前，我们应该明白过程控制的目标是什么。

图 16-6 所示为一个工厂过程和现场总线解决方案的案例。图中左边的输入管道基于上游过程操作以某个填补率对水箱进行注水。该系统的目标是通过控制输出流来保证罐内液位始终保持在一个给定的范围之内。控制器通过现场总线从液位变送器获得水箱的水位，并通过现场总线将阀位值发送给阀门。在很多过程工厂中，罐内液位超过其上限或下限值将会造成极大的损失。

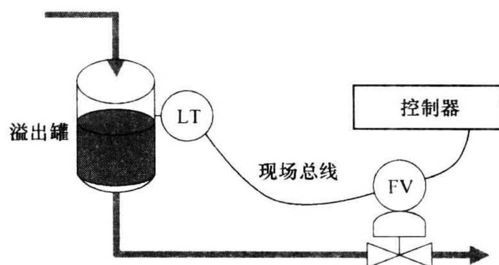


图 16-6　基于现场总线的罐内液位控制

图 16-7 采用了传感器网络来达到相同的目的。这里的挑战是我们是否可以通过在现场设备中使用更多的传感器以及采用当前和将来的传感器网

络技术来获得比图 16-7 中的系统更好的性能。我们可以在下一代现场设备中实现额外的或冗余的测量，例如流量和上游压力测量可以作为控制阀的一部分。或者新的控制模式也可能出现。

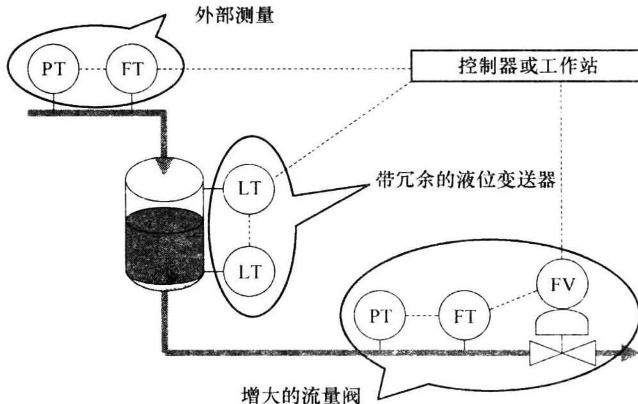



图 16-7 基于传感器网络的罐内液位控制

人们正在非常努力地尝试在工业过程控制中使用无线技术。无线技术在目前的流程控制系统中主要用于监测。该领域仍然面临着很多大家公认的问题和挑战。然而，从长远来说，主要的挑战还在于如何把无线传感器网络用于控制。工业界和学术界对解决这些问题的持续、共同努力将会带来显著效果。

## 16.2 改进使用不稳定通信技术的 PID 控制

在标准工业过程控制系统中，控制回路中的功能块是周期性执行的。也就是说，传感器以固定速率向控制功能块提供采样数据；控制功能块在相同速率下根据输入做出相应的计算，并向执行器发送控制命令。这种模式可以很好地运行于稳定的有线网络，例如 Fieldbus 和 PROFIBUS。然而，部分有线网络可能会被无线网络所取代。无线网络可能会有间歇性地通信丢失，这一假设也是很合情理的。在本章中，我们首先确定在通信丢失的情况下，标准 PID 算法的恶劣动态响应；然后，提出一种增强型 PID 算法，以改善通信丢失时的动态响应。当没有通信丢失时，增强型 PID 功能块与标准 PID 功能块的功能完全相同。当通信丢失时，增强型 PID 功能块内部集成的组件可以补偿丢失的数据。当通信连接恢复后，增强型 PID 功能块中的派生组件，能够消除输出中可能存在的尖峰值。我们在多个无线应用场景下对增强型 PID 算法进行了评估。实验结果证明了增强型 PID 算法拥有诸多优势（Chen 等，2006）。

### 16.2.1 控制环路

传感器能够提供一些物理特性的测量值和状态属性，例如，管道中与工业过程相关的流体。控制器根据传感器的测量结果，对执行器做出适当调整，从而将工业过程维持在目标值附近（例如维持在设定值附近）。控制回路以足够快的速率周期性执行，这样足以校正工业过程中任何不期望出现的偏差。

因此，不稳定的通信连接对标准控制模式而言是一个不小的挑战。现在，我们来考虑带有无线信道输入的 PID 功能块。假设无线信道输入在 $t_1$ 时刻丢失，又在 $t_2$ 时刻恢复连接。PID 中的微分环节可能会在 $t_2$ 时刻引起输出尖峰。此外，从 $t_1$ 时刻到 $t_2$ 时刻，复位组件可能会由于 $t_1$ 时刻存在的误差而终结。

在本文的研究中，我们将研究重点放在应用最为广泛的控制功能块——PID 功能块上。我们修改 PID 算法中的积分和微分运算，以检测通信的丢失并主动对其补偿。多种无线场景下的仿真结果证明了增强型 PID 算法的优越性。

### 16.2.2 标准 PID 算法

PID 是工业过程中最常用的控制算法。如图 16-8 所示，控制器对过程变量（PV）与参考设定值（SP）进行比较，将得到的误差值用于计算新的输出值，该输出值可以使 PV 值恢复到其期望参考设定值（SP）。

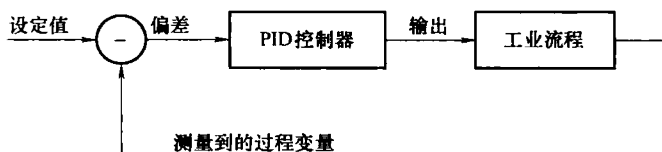



图 16-8　PID 功能块

PID 代表算法中的比例、积分和微分组件。三个组件分别完成不同的任务，对系统功能也有着不同的影响，其输出累加起来产生系统的输出。

虽然 PID 算法中有多个变量，但是标准 PID 算法在无速率限制的非交互形式、所有控制组件都基于偏差条件下的公式为

$$\text{Output} = K_P\left[e(t) + K_I\int e(t)\,d(t) + K_D\frac{de(t)}{dt}\right]$$

式中，$K_P$、$K_I$ 和 $K_D$ 分别是比例、积分和微分的增益。

数字式 PID 算法的软件实现是基于采样数据周期性的产生过程变量（PV）。

在没有通信丢失的情况下，PID 算法在被配置后将控制对应的工业过程，并将其维持在稳定状态。图 16-9 显示了 PID 算法对过程扰动的反应。

$t_0$ 时刻之前，PID 输出（out）保持恒定，过程变量（PV）值也维持在设定值

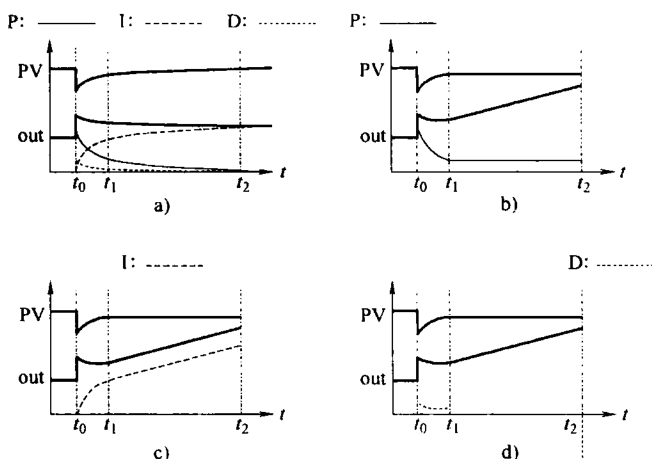



图 16-9 输入丢失的标准 PID 功能块

（SP）上。在 $t_0$ 时刻，由于过程扰动的影响，PV 值有一定的下降。为校正该下降，PID 增加其输出。在 $t_2$ 时刻，PV 值恢复到 SP；输出（out）也稳定下来了，但是其稳定值略大于其常态值，以便对扰动进行补偿。如图 16-9a 所示，输出（out）是比例（P）、积分（I）和微分（D）三者之和。

#### 16.2.2.1 输入通信丢失

如果传感器发出的输入通信在 $t_1$ 到 $t_2$ 时刻之间发生了丢失，那么 PID 控制器中的各个组件对输出（out）会产生什么样的影响？如图 16-9b，c，d 所示，对于 PID 功能块，在这段时间的 PV 测量值与 $t_1$ 时刻的值相同。

图 16-9b 所示为比例（P）增益。由于 PV 和 SP 的测量值保持恒定，所以比例增益在 $t_1$ 到 $t_2$ 时刻也保持恒定。图 16-9c 所示为积分（I）环节。由于过程变量（PV）和参考设定值（SP）保持恒定，PV 与 SP 之间的误差也保持恒定，所以积分环节在 $t_1$ 到 $t_2$ 时刻之间为一条线性增加的直线。图 16-9d 所示为微分（D）环节。由于 PV 和 SP 保持恒定，偏差值恒定，所以微分环节在 $t_1$ 到 $t_2$ 时刻之间为 0。因此，如图 16-9b，c，d 所示，PID 功能块的输出（out）在 $t_1$ 到 $t_2$ 时刻之间为一条线性增加的直线。这将导致系统不稳定。通信丢失时间越长，PV 与 SP 之间的偏差将越大。

一旦通信连接在 $t_2$ 时刻恢复，PID 控制器将会回归到正常状态。$t_2$ 时刻的微分计算是基于 $t_2$ 时刻的 PV 测量值以及 $t_2$ 时刻之前一段周期的 PV 测量值之间的偏差。因为 $t_1$ 时刻的 PV 值可能会被涵盖在 $t_2$ 时刻之前一段周期的 PV 值内，所以微分计算部分可能会出现尖峰输出。$t_2$ 时刻的 PV 值可能与 $t_1$ 时刻的 PV 值差别巨大。由于 PV 值在 $t_1$ 到 $t_2$ 时刻之间会发生变化，这样微分尖峰值可能会更大。由于比例

和微分环节的突变，输出值在 $t_2$ 时刻之前和之后都将会有较大的脉冲波动。

#### 16.2.2.2　输出通信丢失

如果输出通信在 $t_1$ 时刻到 $t_2$ 时刻之间发生丢失，我们进一步分析标准 PID 控制器将做出何种动作。此处我们假设没有其他干扰，并且输入通信正常。

如果输出通信在 $t_1$ 时刻到 $t_2$ 时刻之间发生丢失，执行器从 $t_1$ 时刻开始将保持 $t_1$ 时刻的输出值不变直到 $t_2$ 时刻，并在 $t_2$ 时刻接收 PID 控制器发出的新输出值。P、I、D 组件的运算都是基于当前 PV 值的。如图 16-10b，c，d 所示，这将使 PV 测量值逐渐达到设定值 SP，并略微超过该设定值。这正是我们所期望的 PID 理想状况。唯一的缺陷是执行器的输出值在 $t_1$ 时刻到 $t_2$ 时刻之间会出现突起波动。

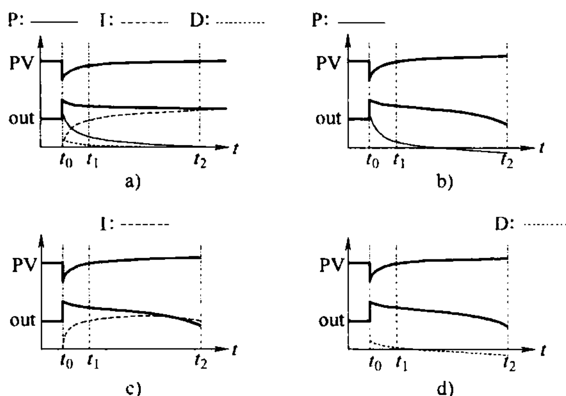



图 16-10　输出丢失的标准 PID 功能块

#### 16.2.2.3　输入输出通信全部丢失

如图 16-9 所示，当输入和输出通信全部丢失时，PID 的行为与只有输入通信丢失时相同。唯一的差别在于，当通信在 $t_2$ 时刻恢复时，实际 PV 值有所不同。当输入和输出通信全部丢失时，实际 PV 值偏移较少，而执行器输出保持恒定。类似地，执行器输出值也有突起波动。

### 16.2.3　增强型 PID 算法

对于上文提到的 PID 算法的数字化实现，其基本假设是该算法周而复始地执行。当包含测量值的输入丢失时，执行计算复位操作可能不是很恰当，因为微分计算环节获取新测量值后可能会在输出中产生一个尖峰。如果使用之前过程的值继续执行 PID 功能块，输出值将会继续变化。该变化依赖于复位设定值，以及最后过程测量值与设定值之间的偏差值。如果只有当有新的测量值传送时才执行控制功能块，那么就可能会延迟控制器对设定值变化的响应，以及前馈控制对测量扰动的响

应。此外，当执行控制时，根据预定的执行周期或从上一次计算复位开始来计算新的复位时间，可能会导致过程可变性的增加。

当测量值不是被周期性地更新时，为了提供最好的控制性能，PID 控制器需要从最后一次测量值更新开始被重构，以便反映期望过程响应中复位和微分环节的作用。图 16-11 描述了这样的一种实现方式。

如图 16-11 所示，复位/比例作用值（PID 中的积分/微分环节）可以基于通信中的新值标志来确定。当收到新的测量值时，滤波器输出可以通过如下公式计算得到过程响应，即

$$F_N = F_{N-1} + (O_{N-1} - F_{N-1})\left(1 - e^{\frac{-\Delta T}{T_{\text{Reset}}}}\right)$$

式中，$F_N$ 为新的滤波器输出；$F_{N-1}$ 为上一执行过程的过滤器输出；$O_{N-1}$ 为上一执行过程的控制器输出；$\Delta T$ 为传送新值所消耗的时间。

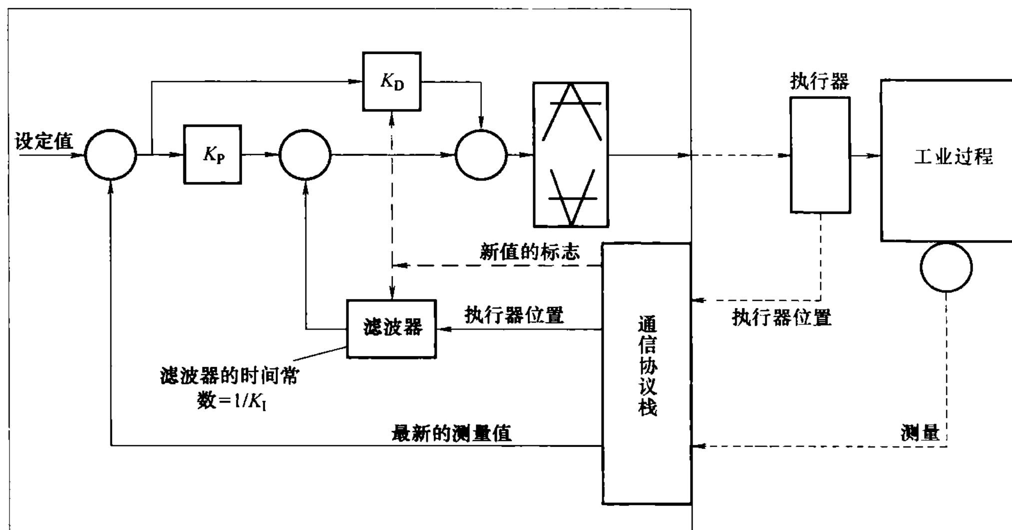



图 16-11　增强型 PID 算法的应用

由于上次传输执行器位置信息反映在反馈执行器位置中，这样就可以自动补偿传输到下游元件中的任何输出损失。

本例中的微分部分（未使用比例限制）可以由以下公式计算得到：

$$O_D = K_D \frac{e_N - e_{N-1}}{\Delta T}$$

式中，$e_N$ 为当前误差值；$e_{N-1}$ 为前一次测量误差；$\Delta T$ 为传送新值所消耗的时间；$O_D$ 为控制器的微分环节。

现在，我们来考虑当丢失几个周期的输入时，微分环节所产生的作用。当通信

恢复时，上面公式中的 $e_N - e_{N-1}$ 对原算法和修改后的算法而言都是相同的。然而，对于标准 PID 算法，微分环节中的除数为时间周期，而在新算法中，该除数变为成功接收到两次测量值的时间间隔。可以明显看出，改进后的算法所产生的微分动作与标准 PID 算法相比要小些。

标准 PID 算法处理通信丢失问题时将面临两个主要问题：①通信丢失后算法的继续执行；②通信恢复时输出中的突变。增强型 PID 算法通过以下方法能有效地解决上述问题：通信建立时仅仅计算积分和微分环节，并且将执行器的反馈包含到复位计算中。

## 16.2.4　实验与结果

我们设计了多个实验来验证新算法的正确性。首先，实验结果证明当通信稳定可靠时，新算法与常规算法的输出结果相同。然后，当通信不稳定时，实验结果证明新算法比现有的 PID 算法具有更好的响应特性。

### 16.2.4.1　实验装置

我们设计了两个简单的 PID 控制回路，如图 16-12 所示。

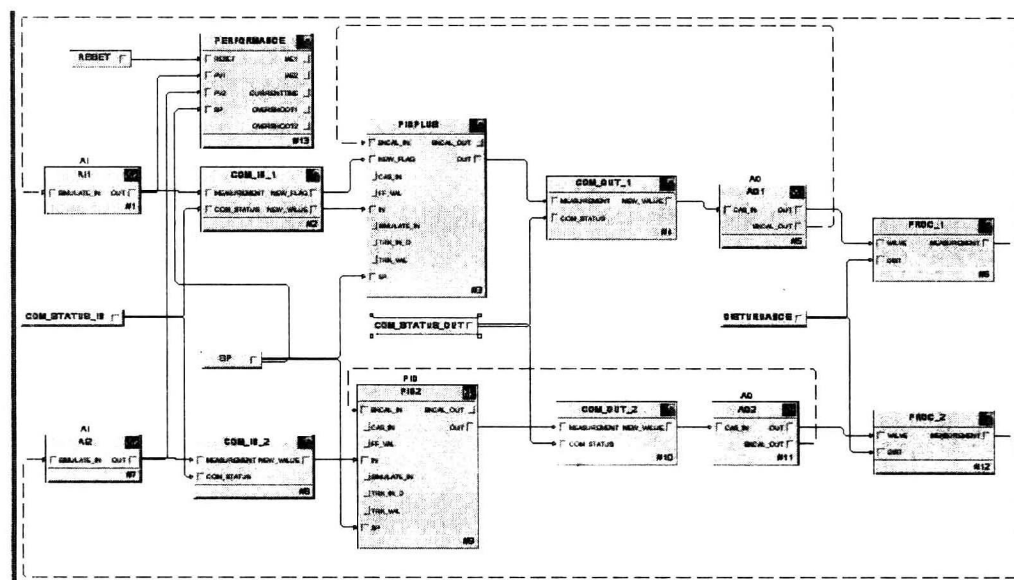



图 16-12　实验装置

PROC_ 1 和 PROC_ 2 是两个相同的过程，两者均含有一个具有 1s 时延的二阶过程，其时间常量分别为 6s 和 3s。

功能块“PIDPLUS”用于改进型 PID 功能块，功能块“PID2”为标准 PID 功

能块。整定应用程序可以被用来测试功能块“PID2”以确定其参数，建议其增益设置为0.85、复位值为10.71、比例为1.71。功能块“PIDPLUS”的整定参数与功能块“PID2”的整定参数都被设置为相同值。功能块“PIDPLUS”可被配置成在复位环节中利用BKCAL_ IN的值。

过程变量的传输可以通过COM_ STATUS_ IN控制的COM_ IN_ 1和COM_ IN_ 2功能块来仿真。如果COM_ STATUS_ IN被设置为1，那么COM_ IN_ 1和COM_ IN_ 2功能块就能够精确地传送测量值。否则，这两个功能块将丢弃测量值。相同的逻辑关系也可应用于COM_ OUT_ 1、COM_ OUT_ 2和COM_ STATUS_ OUT输出功能块中。

通过改变外部设定值，并且引入一些对各个PID和相关过程影响相同的扰动，我们就能够评估出功能块“PIDPLUS”和功能块“PID2”的表现性能。PERFORMANCE功能块汇集了功能块“PIDPLUS”和功能块“PID2”的表现性能。此处用到的矩阵为积分绝对误差矩阵（IAE）。

所有功能块的扫描速率都被设定为0.2s。初始时，过程中的不可控扰动（DISTURBANCE）被设定为20。

#### 16.2.4.2 可靠通信

状态值COM_ STATUS_ IN和COM_ STATUS_ OUT都被设置为1意味着通信是可靠的。在本次仿真中，状态值COM_ STATUS_ IN和COM_ STATUS_ OUT都被设置为1，设定值（SP）的值由50变为60。图16-13中的左边部分显示了相应的仿真结果（从时刻11:10到11:11）。

曲线AI1/OUT.CV与曲线AI2/OUT.CV匹配良好，曲线AO1/SP.CV也与曲线AO2/SP.CV匹配良好。由此，我们可以推断出在通信可靠情况下这两种功能块的工作性能相同。

#### 16.2.4.3 不可靠通信

为了研究通信的不可靠性对这两种功能块的影响，我们考虑以下两种情况：不可靠输入和不可靠输出。

1. 不可靠输入

在输入丢失期间，最后一次传输来的过程变量会被保存起来并被用在PID功能块中。我们首先通过改变设定值来观察实验结果。图16-13右侧部分显示了相应的实验运行结果，其中SP由60下降到50。

在输入信道被关闭后，SP与输入给PID功能块的过程变量之间的误差值也保持恒定。对于功能块“PID2”（即标准PID功能块），积分环节的持续累加作用导致了AI2/OUT和AO2/SP值的线性减少。然而，由于功能块“PIDPLUS”（即增强型PID功能块）有通信丢失标志，所以功能块“PIDPLUS”能够在通信丢失期间冻结复位组件，从而致使AO1/SP的值平稳变化。由于AO1值是恒定的常量，所

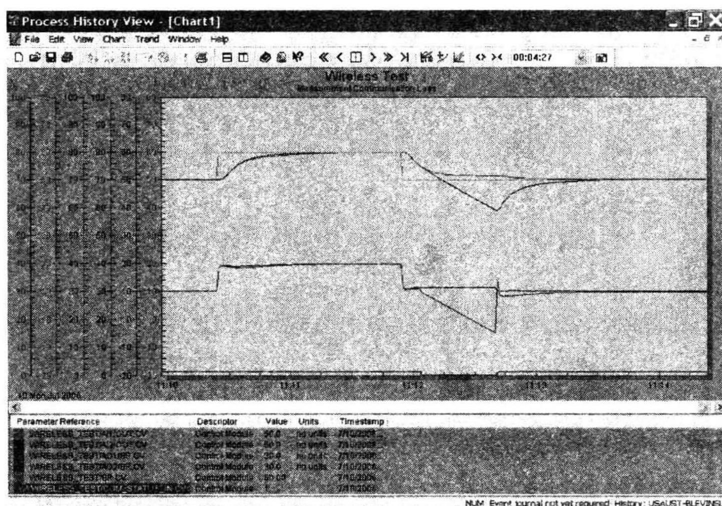



图 16-13　输入丢失并且设定值变化

以如 AI1/OUT 曲线所示，过程变量 PROC_ 1 逐渐地接近设定值。

在通信恢复后，输入到功能块“PIDPLUS”和功能块“PID2”的过程变量分别反映了 AI1 和 AI2 提供的真实测量值。对于功能块“PID2”而言，其 AI2/OUT 值比 SP 低许多。在通信恢复时，由于功能块“PID2”微分环节的作用，AO2 中将出现一个尖峰值。对于功能块“PIDPLUS”而言，其 AI1/OUT 值与设定值相近，两者间的微小偏差再经过新算法的微分环节中的除数因子就被进一步均匀化了。因此，AI1 和 AO1 都可以平稳地过渡到其稳定状态。

这两种 PID 功能块之间的差异还可以通过功能块的性能参数来进一步展现出来。在 121s 的时间间隔内，功能块“PIDPLUS”的积分绝对误差（IAE）为 169，而功能块“PID2”的积分绝对误差（IAE）为 372。

我们也测试了不可测扰动对这两种功能块的影响。在该实验中，扰动值 DISTURBANCE 由 20 增加到 30，对应的仿真结果曲线如图 16-14 所示。功能块“PID2”的性能与图 16-13 中显示的相同，也可用解释该图的原因解释。对于功能块“PIDPLUS”，在通信丢失期间，复位组件维持恒定。因此 AO1 保持相同的输出值，反过来产生相同的 AI1 值。通信输入恢复后，PIDPLUS 开始改变其输出值（AO1/SP），使 AI1/OUT 值回到设定值。在时间周期内（196s），功能块“PIDPLUS”的 IAE 为 333，而功能块“PID2”的 IAE 为 366。

2. 不可靠输出

这种情况下，我们也从以下两个方面来检测 PID 功能块的性能：SP 的变化和不可测扰动。

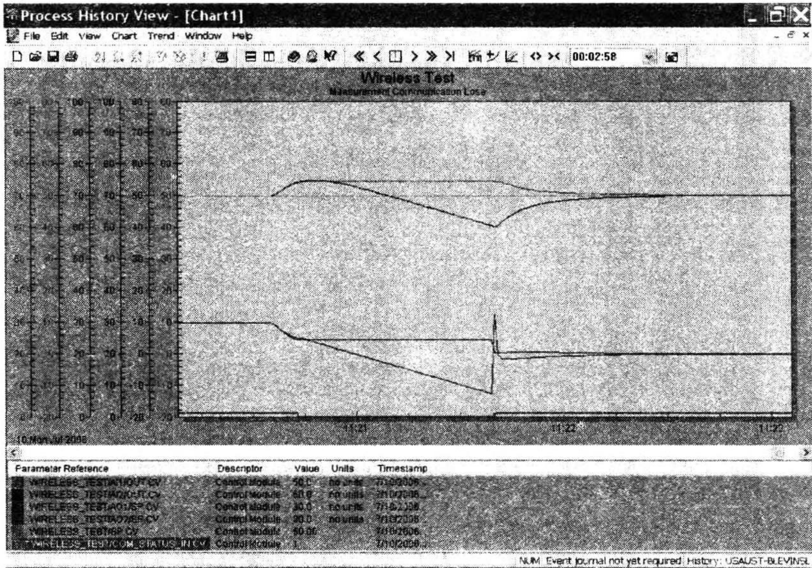



图 16-14　输入丢失且扰动不可测量

当 SP 变化以及通信可靠时，我们首先将 SP 由 50 变为 60。然后，当过程稳定在 SP 的值为 60 时，再将 SP 的值改变为 50，并且切断输出信道。图 16-15 显示了相应的仿真结果曲线。

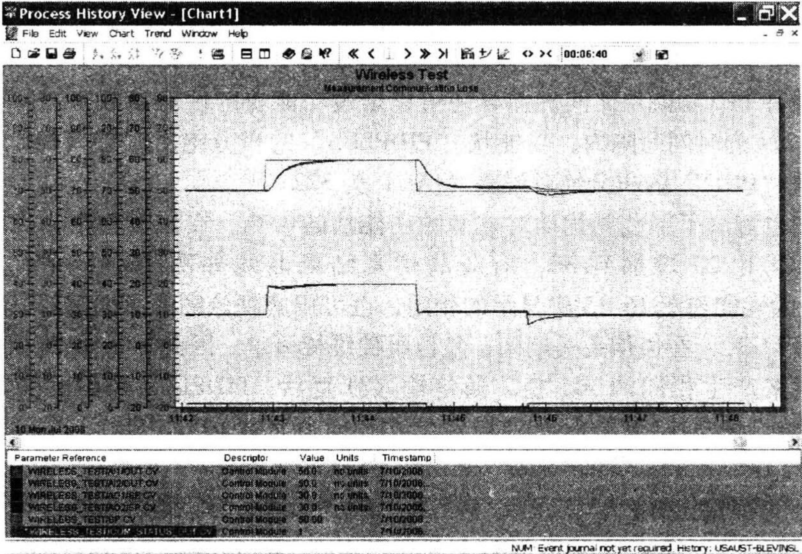



图 16-15　设定值变化引起输出值丢失

如图 16-15 所示，通信丢失后，功能块“PIDPLUS”与功能块“PID2”的输出相等。由于这两个受控过程相同，所以 AI1. OUT 和 AI2. OUT 值的变化趋势也相同。通信恢复后，虽然功能块“PIDPLUS”和功能块“PID2”的输入误差相同，但是功能块“PIDPLUS”中微分环节的除数因子远大于功能块“PID2”中的除数因子，因此曲线 AO2/OUT 会出现一个尖峰值。在转换期间，功能块“PIDPLUS”的 IAE 为 190，而功能块“PID2”的 IAE 为 196。

我们再一次向过程中引入不可测量扰动，用以检测这两种功能块。在该实验中，扰动变量 DISTURBANCE 的值由 20 变为 30。相应的仿真结果如图 16-16 所示。

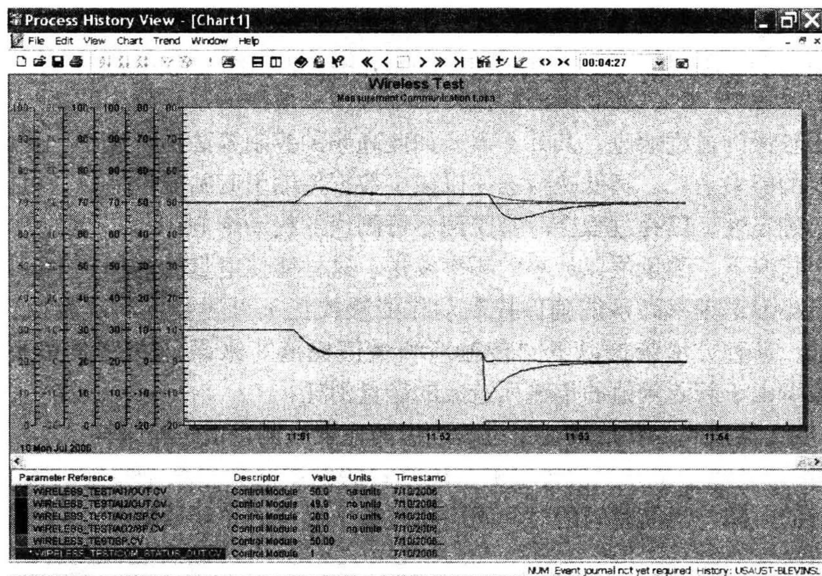



图 16-16　输出丢失且扰动不可测

图 16-16 中的曲线与图 16-15 中的曲线相似，也可以用上文中提到的方式解释。此外，对比图 16-16 与图 16-15 会发现，图 16-16 中功能块“PIDPLUS”相对于功能块“PID2”的改进比图 16-15 中的改进更加明显。这是因为，在通信恢复时，图 16-16 中功能块“PID2”的输入误差大于图 16-15 中的输入误差。在图 16-16所示的转换周期内（158s），PIDPLUS 的 IAE 为 267，而功能块“PID2”IAE 为 388。

## 16.2.5　减少数据吞吐量以增加电池寿命

如上所述，我们已经讨论了如何增强 PID 功能以应对不可靠通信。无线网络可能会发生通信不可靠的情况。另一方面，无线网络需要减少数据吞吐量以节省电池

电量。为达到该目的，在不影响控制性能的前提下，我们可以主动停止输出传输（chen 等，2005）。当数值不变化或变化很小时，我们可以停止数据传输，增强型 PID 算法会将其理解为数据丢失，如上述所知，此时的输出结果与过程值变化较大，但与通信丢失时相比变化不大。

为减少数据传输中的能量消耗，最好的办法是最小化测量值的发送频率。然而，为避免测量值与控制运算之间的同步而带来的限制，大多数多回路控制器过于频繁的对测量值进行采样，实际采样值通常是图 16-3 中所示的 2～10 倍。

正如基于 FF 的现场总线设备所做的那样，将测量值和控制执行同步起来，这样就不再需要过于频繁地对测量值进行采样。然而，如果在调度控制中使用传统的处理方式，即控制算法的执行频率是过程响应的 2～10 倍，当工业过程中有多种不同速率的过程响应时，控制算法的执行频率应该是最快的过程响应的 2～10 倍。这样，对于较慢的过程响应，其并不需要如此高频的控制算法执行速率，从而引起了没有必要的能量消耗。降低执行速率以减少数据传输引起的能量消耗，可能会增加控制的不确定性，因为过程会时常受到不可测量的扰动影响。

理想状况下，测量值以最小的频率发送，这样能使电量的消耗减少到最小。测量值的最小发送频率必须能确保控制动作能够校正不可测量扰动或者操作点的变化。例如，某种方法依据以下"传输新测量值规范"来设计变送器和无线通信，从而能减少由于新测量值的传输而造成的能量消耗：

1）变送器以 4～10 倍快速于过程响应的速度对测量值进行采样。

2）如果新测量值和上次传输测量值之间的偏差值大于某个特定的幅度，或者上次传输的时间与当前时间的时间间隔超过某个设定的更新周期时，那么新测量值将会被传送。

对于本例中用到的滞后过程，当无线传输遵循上述规则时，测试期间的采样值传输次数减少了约 96%。利用应用于无线通信的改进型 PID 算法，非周期性测量值更新对控制性能的影响能被最小化。表 16-1 以 IAE 的形式列出了测量值周期性更新与非周期性更新对控制性能影响的差异。

**表 16-1 控制性能差异**

| 传输方式/控制方式 | 传输数目 | 积分绝对误差（IAE） |
|---|---|---|
| 周期性传输/标准 PI 控制器 | 692 | 123 |
| 按照通信规范传输/无线 PI 控制器 | 25 | 159 |

控制规范和对 PID 控制器的修改应用到无线变送器上之后，变送器必须提供的用于传输数据的电流将大幅减少。能量需求的减少又增加了无线变送器控制应用的数目。

### 16.2.6 评论

利用执行器反馈来实现平滑输出转移，这并不是一个新观点。基金会现场总线（FF）标准已经定义了反算输入输出（back-calculate-in/out）连接，用以在系统的启动阶段提供平滑转移。某些控制系统在系统启动完成后，仍然继续使用该连接。

现代控制系统中的 PID 功能块有针对数据值的标志位。这样，某个数据值可以被标定为通信丢失状态。一些系统能够利用这个标志位来提供故障保护机制。例如，基金会现场总线（FF）标准允许有限数量的通信丢失，此后会产生错误警告并且功能块将进入错误状态。这样反过来就可以在通信丢失期间将功能块强制转化为手动模式。这种方法能够缓解但并不能完全消除通信丢失带来的问题。前文中提出的针对 PID 通信丢失的改进方法，其不同之处在于，我们明确地处理了通信中发生的错误，并且利用了一些相关的信息。

目前的控制器设计是在假设周期性采样的前提下做出的。然而，该假设在无线环境中并不成立。当通信稳定可靠时，增强型 PID 算法与标准 PID 算法执行效果相同。但当检测到有通信丢失时，增强型 PID 算法则可以去除输出中可能产生的尖峰，使输出值更加平滑。

# 第 17 章　实时无线网状网络的研究

摘要：诸多研究机构针对无线网状网络做了大量的研究工作。它们中的许多研究都是理论上的，研究结果的验证是通过模拟或在有限的测试环境中实现的。无线网络在工业环境（特别是过程工业）中的应用正得到越来越多的关注。不同于办公室或住宅中的移动自组织网络，过程工业中的无线网络必须满足实时性要求，有时甚至还必须满足“硬”实时要求。在“硬”实时系统中，一次超时就可能产生灾难性的后果。实时或嵌入式应用被认为远比基于 PC 的应用难。同样，实时无线网络也非常难。无线网状网络从研究阶段到实际工业应用的时机已经成熟。这本书中的许多主题都值得学术界的进一步深入研究。本章将再次强调其中的一些主题。无线技术给过程控制行业带来了一些额外的附加值。反过来，过程控制行业接受了无线技术，这也加快了无线技术的发展。过程工业环境为研究机构在过去十年中提出的任何理论和方法，提供了一个真实的测试环境。

## 17.1　实时系统

实时系统的特点不是它的速度，而是其确定性行为。通常，过程控制回路的运行周期为 1s 或小于 1s，其关键要求是一个完整的控制算法必须在每个运行周期内被执行完毕。快速但迟到的响应比慢但及时的响应更差。离散制造控制系统的运行周期可能是微秒级的。与离散制造控制系统相比，过程控制系统的运行速度要慢些；但是，过程控制系统中的实时性问题与离散制造控制系统的实时性问题一样重要和复杂。

实时系统通常不断重复地执行同一作业。每次重复作业必须被及时地完成。实时研究领域存在一个很常用的实时任务模型。在该实时任务模型中，实时任务 $T$ 是一个三元组 $\{C, D, P\}$，其中 $C$ 是执行时间，$D$ 是相对期限，而 $P$ 是周期。在每个周期 $P$ 的开始，任务 $T$ 请求一段时间长度为 $C$ 的执行时间，并且该任务应该在时间长度为 $D$ 的相对期限内被执行完毕。每次请求被称为一个作业。通常情况下，$D$ 小于或等于 $P$。如果任务 $T$ 的任何作业错过了截止日期，那么任务 $T$ 就失败了。一个实时任务集 $S$ 是 $n$ 个实时任务 $T_1$，$T_2$. . . ，$T_n$ 的集合。如果任务集 $S$ 中的任何一个任务在某个调度策略的控制下都不会错过截止日期，那么该任务集 $S$ 是可被该调度策略调度的。如果任务集 $S$ 可以由至少一个调度策略来调度，那么该任务集 $S$ 就是可行的。实时研究领域中也存在有许多其他实时任务模型。例如，某个任

务可能有固定的起始时间。在一些简单的实时任务模型中，任务的截止时间等于其周期。对于一些连续实时应用，其任务通常是不断重复执行的，因此任务的定义包含有周期域。*P* 有时候也被称为最小间隔时间以定义不严格按周期重复的任务。很多任务调度的结论在 P 被解释为最小间隔时间时也成立。

基于单处理器的实时任务调度研究如今被认为是成熟的了（Chen 等，1997；Chen，1999；Chen 等，2003；Kuo 和 Mok，1991；Liu 和 Layland，1973；Sha 等，1990；Sha 等，1994；Stankovic 等，1998）。现实工业应用已经使用了许多著名的实时任务调度策略，例如最早截止时间优先（Earliest-Deadline-First，EDF）、单调速率调度算法（Rate-Monotonic-Algorithm，RMA）和优先级顶置协议（Priority-Ceiling-Protocol，PCP）。基于多处理器的实时任务调度研究也取得了很多成果。在多处理器的实时任务调度中，任务可以被选择性地运行于系统中的任何处理器。

## 17.2 值得研究的领域

1. 安全

有人说，安全方面的问题对无线技术应用于过程工业而言可能是一个大的障碍。如本书第 8 章所述，WirelessHART 系统包含了大量的安全功能。如今，安全方面的问题对于任何过程工业应用而言都可能是一个大的障碍。因此，从某种程度上讲，仅对无线技术提及安全方面的问题是不公平的。无线系统面临的任何安全问题，在有线系统中同样存在，唯一的区别在于成本和严重程度。当我们讨论安全问题的时候，我们应该讨论整个过程工业车间的安全，无线通信仅仅是其中的一部分。有线控制系统有两个最好的防御：其一是其专有的本性；另外一个是其与互联网不相连。系统的专有性又会降低系统的影响力和受欢迎程度；有线控制系统与互联网的不相连能使其可以避免在线攻击。诚然，无线使得安全研究更紧迫和更有趣。例如，如何利用有限的存储空间来实现包含了椭圆加密算法的公开/私有密钥机制？如何用能力有限的处理器完成复杂的加密算法？

2. 端到端的延迟

分布式网络上运行的实时应用可被建模成：每个节点中的实时任务集以及节点间的实时数据通信。源节点和目标节点之间的实时数据通信可被考虑成：源节点中的一个实时任务、目标节点中的一个实时任务，以及时间同步需求。每个通信任务都有一个执行时间、一个相对截止时间和一个周期。执行时间是通信的传输时间。源节点发送数据时，目标节点必须处于监听模式。一旦我们能将每个节点中的问题分成多个独立的调度问题，那么这些独立的调度问题也就可以形成一个任务集。幸运的是，我们通常总能找到办法来调度这个任务集。因为一些主流分布式网络（如因特网）通常采用“尽力而为”的数据传输机制，所以这类网络只能提供有限

的实时性应用。而且，这类网络也很难提供有保证的数据报传输。

如果源节点与目标节点不是直接邻居，这将会带来另一个挑战。在这种情况下，从源节点到目标节点路径上的所有节点都应该及时地将数据传递到下一跳，这样总延迟才将不会超过通信的相对期限。由于路径上的每个节点都独立地工作，所以节点很难依据之前的传输延迟来动态地调整其发送时间。一个更简单的办法是预先设定每个节点的延迟，其对应的解决方案是给每个节点预先分配各自的时延。例如，在 RSVP 中，带宽和时延的请求被从源节点传递到目标节点。每个中间节点都返回其承诺能提供的带宽和时延范围。然后，每个节点最终承担的份额将会被计算和分配。为了确保实时性，某种程度的集中控制是必需的。

已经有大量的研究工作用于发现满足 QoS 要求（如延迟边界）的数据路径。这些研究结果既可适用于集中式网络，又可适用于分布式网络。例如，在差异启发式时延约束最低成本（Delay-Constrained Least-Cost，DCLC）单播路由算法中，源节点到其他节点的路径是通过网络图的广度优先或深度优先搜索而确定的。由于在线执行 DCLC 算法的代价将会是非常昂贵的，所以对于周期性的实时应用，我们可以使用离线 DCLC 算法，也可以在应用程序执行期间应用 DCLC 算法的在线结果。

3. 可靠性

无线网络面临的可靠性问题比有线网络更突出。WirelessHART 标准采用各种方式来解决这一问题。请参阅本书第 10.9 节。随着无线技术在过程工业的大规模应用，将会出现更多令人感兴趣的与可靠性相关的问题。

4. 故障语义

因为故障总是不可避免的，所以故障恢复也是一个很有趣的研究点。我们需要针对无线网络定义一些故障语义，为它们有效的处理错误提供一个理论框架。

5. 统计

无线网状网络中存在着许多不确定的事物。研究机构正在积极地研究如何用统计方法来处理这些不确定事物。流程控制应用又给这些研究公式添加了另一个度量——实时性，以及如何从不确定的事物中获得一些确定的保证。

6. 集群网

一些研究工作已经开始关注大规模无线传感器网络，即集群网。集群网是一系列小型网状网络汇集而成的网络，是无线技术在过程工业应用中的一种自然模式。WirelessHART 网络最适用于位置固定的设备，而 Wi-Fi 网络最适用于移动的工人。我们可以将 WirelessHART 网关接入到 Wi-Fi 网络，这样就可以充分利用这两种网络各自的优点。针对这种分层式拓扑结构的研究也能让工业界获得直接的受益。

7. 电池方面的考虑

在无线传感器中，电池的使用存在着两个研究领域：一个是电池本身的设计；另一个是如何最大限度地延长电池的使用寿命。

# 第 18 章　工业无线系统和 WirelessHART 标准的未来

摘要：本章由四个部分组成。在第 18.1 节中，我们讨论一些工业无线系统的优势，以及在什么地方可以用无线系统取代已存在的有线系统。此外，我们也列出一些有线系统没有涉及或很少涉及的新应用。在第 18.2 节中，我们讨论位置感知应用和技术。将来，位置跟踪将是工业无线应用的一个重要组成部分。本小节还介绍一种利用 WirelessHART 系统实现位置测定的应用。第 18.3 节谈到物联网。无线传感器网络在物联网中可以作为对物理世界的直接接口。第 18.4 节揭示工业无线的未来发展方向，并提供一些关于 WirelessHART 标准将如何演变以满足这些未来发展方向的想法。

## 18.1　过程自动化中的无线传感器网络

如今，数以百万计的 HART 设备已经被部署在工业现场，其中只有一小部分 HART 设备被数字式地连接到上位机以提供过程数据以外的数据。有了 WirelessHART 标准，用户可以给已经存在的或新的系统添加无线功能。无线解决方案在现场设备、控制系统、资产管理软件包之间提供了灵活性、可扩展性、互操作性。同时，WirelessHART 技术依靠低功耗、低数据率的无线通信将许多小型传感器互联起来。随着大量新环境数据的出现，我们可以不断地探索潜能以提高过程控制的质量。WirelessHART 技术还可以为用户的操作提供无线连接，并能够利用智能现场设备提供的信息来提高生产力。

展望未来，无线系统可以被用来取代工业现场中的有线系统，也可以被用于全新的应用。接下来，我们从总体上讨论工业无线涉及的新应用以及工业无线产品。

### 18.1.1　工业无线涉及的新应用

1. 资产管理

设备故障以及相关的维修通常会花费很多时间和金钱，还会减少工厂的产量和可用性。小问题如果未能被及时发现，就可能演变成引起重大损失的大问题。这样，一次小的维修任务就可能演变成一次重大的维修任务，从而减少资产设备的使用寿命或需要更换资产设备。随着工业无线网络的使用，资产设备的健康情况可以被不间断地监测。这样，小问题就可以被及时发现和消除，从而可以延长资产设备

的使用寿命。

2. 效率

工厂效率的提高能降低产品的原材料成本，并且能提高产品的产量。效率的少许提高也可以为工厂利润带来实质性的改善。智能无线解决方案可以高性价比地增加所需的额外测量，从而能用来优化工厂的效率。这些额外的测量点可以涉及我们过去不可能监测的对象，例如移动或旋转的设备，或在恶劣环境中的监测对象。

3. 维护

工厂资产的维护是可扩展的。大多数工厂仍然依赖于预防式或被动式的维护方法，即使这些方法会降低工厂资产的可用性。智能无线解决方案可以帮助实现预测式和主动式的维护方法。

4. 安全

智能无线解决方案可以实现安全设备（如洗眼工作站）的无线监控，以便尽早地采取行动来防止事故的发生。我们也可以在工厂的危险区域无线监控仪表数值，以减少工作人员的安全风险。

5. 环境

通过提供快速警告和对环境漂移的精确记录，无线技术可以最大限度地减少危险、清理以及环境释放的代价。

### 18.1.2 工业无线产品

现在，我们来关注过程数据从现场设备到终端用户的传输路径。在过程控制系统中，工业无线产品可以存在于从现场设备到数据接收站的各个级别的产品中。现场设备可能有内置的无线发射器，或者通过有线连接到一个无线传输节点。这个无线传输节点能与某个无线控制器/工作站通信，或者能与连接到控制器/工作站的另一个无线节点相互通信。因此，工业无线产品可用于控制器和工作站之间的通信。然而，更多的无线产品可用于控制系统与其外部世界的通信。

控制单元层的无线产品应该能提供高可靠性的短距离通信。这类无线产品不得不承受恶劣环境的影响，同时可能还有低功耗的要求。区域控制网络层的无线产品要求高数据传输率和长通信距离。虽然它们对数据传输的可靠性要求没有控制单元层的无线产品那样高，但是它们也要求足够高的可靠性。对于区域控制网络层的无线产品，由于其电波涵盖范围更广，所以相关的安全问题开始出现了。在控制系统之外，我们假设任何常规的无线产品都可被用于控制工作站与控制系统的外部世界相互通信。当然，任何与常规无线产品相关的问题也许会涉及更多的问题，我们这里讨论的是如何将其连接到过程控制系统中。

工业无线产品的硬件部分可以是独立的无线收发器，也可以是配备了无线模块的设备和控制器。企业也可以售卖无线部件，诸如天线及配件。无线产品的软件部

分可能是通信协议栈、设备驱动和完整的系统软件。企业还可以提供完整的解决方案，或者帮助客户建立一套工业无线系统。

客户选取无线产品的主要标准是该产品是否能满足自己的需求。选取无线产品的其他标准还包括：产品成本、开发成本、功耗、传输距离、通信的可靠性（网状网络与点对点网络）、带宽、商业化成熟度、项目风险、网络协议、是否支持手持、系统大规模的布置、互操作性、安装工具的支持、故障排除工具的支持、是否支持世界范围内的使用等。

一个未来可能面临的问题是：工业无线产品，特别是在控制网络层的工业无线产品，如何满足过程控制系统的硬实时要求。

1. 无线配件

无线配件包括一些硬件部件，如天线、电缆、配件、基于PC的无线网卡、远程传感器接口等。

2. 无线现场设备

无线现场设备将是市场上最常见的工业无线产品。

3. 网关

网关设备在现场设备与外部世界之间扮演着中间人的角色。网关通常有两种类型：①网关的一端利用现有的有线网络协议与现场设备相连，另一端通过无线方式连接到上位机或其他与上位机相连的中间网关。这种网关的传输距离范围为几百英尺到几英里；②网关的一端是工业无线网络的一部分，另一端通过有线或无线的方式与上位机相连。WirelessHART网关属于第二种类型。

网关可以简单到像一个协议转换器，将数据从一种协议转化成另外一种协议。网关也可以是一种数据接入点，将多个设备的数据汇集起来，使得自己就像一个简单的无线数据源。一些更复杂的网关被称为无线网桥、节点模块或远程终端。它们可以运行软件，也可以被组态配置，还可以处理数据。它们还可以为产品设计师提供了一种透明、简便的手段用来设计无线通信链路。

4. 工业无线网络

目前的趋势是针对工业无线网络的标准化，如WirelessHART标准。

5. 无线控制系统

这将是用于过程控制的最终无线产品。

6. 无线服务

无线服务包括无线电频谱的现场勘测、安装、启动和调试以及培训。此外，无线服务还包括：用于诊断的传感器和数据收集工具、状态检修、资产管理、情况感知、准备就绪的程度以及安全。

## 18.2 位置感知

位置感知是值得特别关注的，因为它对于工厂工作人员的跟踪很重要。当事故发生时，快速的定位和人员营救能使事故的后果有很大不同。随着无线网络被部署于整个工厂，工作人员可以携带能与无线设备交互的手持设备或电子标签，这些无线设备能跟踪该手持设备或电子标签从而定位出工作人员的位置。有理由相信位置感知将会成为工业无线应用的一个重要组成部分。

### 18.2.1 位置感知技术

定位问题被认为是排名前十位的网络问题之一。虽然 GPS 被广泛用于此目的，但是 GPS 定位成本高并且在室内无法工作。因此，非 GPS 定位近来受到了极大的关注。

#### 18.2.1.1 定位的理论原理

定位机制有两种：测距定位和非测距定位。因为非测距定位更关心节点间的关系而不是精确的位置，所以这里不讨论这种定位机制。

通常，定位系统由两部分组成：①坐标已知的参考点；②传感器与参考点之间的关系。这些参考点通常被称为信标或锚节点。目前，三种方法常被用于研究传感器和参考点之间的关系：

（1）RSSI 接收信号强度指示（Received Signal Strength Indication，RSSI）利用信号强度衰减模型来估计发送方和接收方之间的距离。RSSI 面临的问题是当存在噪声或障碍物时其精确性将会受到影响。据悉，在室内环境下，RSSI 的预计精度可以达到大约 10ft（1ft =0.3048m）。

（2）时差 到达时间差（Time Difference of Arrival，TDOA）所利用的是信号的传播速度，这比 RSSI 利用信号衰减的方式更加可靠。然而，由于无线电信号处理对于当前大部分晶振驱动的芯片来说太快了，因此音频信号被替代地用于许多定位系统。此外，到达时间差（TDOA）要求发送方和接收方之间保持时间同步，而这对于许多系统而言都是比较高的要求。

（3）AOA 到达角（Angle of Arrival，AOA）交汇定位法通过阵列天线来确定无线电波的传播方向。这种方法需要一个以上的天线，并利用信号到达各个天线的时间差来计算出无线电波的传播方向。

#### 18.2.1.2 定位技术的属性

（1）物理位置和符号位置信息：物理位置指的是全球位置，如南纬 47°39′17″。符号位置信息包括了一些抽象的概念，如某间办公室的符号位置信息为 5.302。

（2）绝对与相对定位：绝对定位系统为所有定位目标提供一个共享的参考网格，而在相对定位系统中每个节点都可以有自己的参考框架。

（3）本地化的位置计算能力：有些系统需要节点能自己计算出自己的位置，而其他系统利用中央服务器给节点分配坐标。

（4）准确度和精确度：估计出的位置与实际位置之间的定位精度或误码率。

（5）大规模：可扩展性与覆盖范围相关。虽然无线网络可能很小，但是定位机制应该能够覆盖整个网络。

（6）成本：成本可以通过锚节点数量来估计。技术的计算复杂性也会影响成本。

#### 18.2.1.3　定位技术

目前，一些研究机构开发出的定位技术：

（1）利用有趣的环境特点实现节点的定位。该技术利用温度、湿度、环境噪声、频谱能量、接收信号强度等信息来识别出节点的位置（Chen 等，2007）。

（2）充分利用连通性的信息。因为连通性包含了两种情况：连接（正）和非连接（负），所以它可以将空间分成两个部分。利用这些制约因素就可以确定出节点所在的区域（Guha 等，2005 年）。

（3）移动节点的定位。移动模式有几种，我们可以采用顺序蒙特卡罗（Sequential Monte Carlo）定位方法。待定位节点的移动性可以提高定位的精度和降低定位的成本（Hu 等，2004 年）。

（4）一种用来尽可能减小定位最小平方差的迭代方法。迭代算法在定位中是比较流行的。因为一些统计模型没有分析结果，所以迭代程序是求解这些模型的唯一途径。然而，迭代算法比线性编程算法更复杂。因此，迭代算法对于能力有限的传感器而言可能不适合（Liu 等，2006）。

（5）采用一个迭代算法来实现节点的网络部署。因为这样的问题是 NP-hard 问题，我们可以使用近似的方法：弱部署和强部署。这两种部署都提供节点定位不确定性的上限和下限（Basu 等，2006 年）。

（6）使用移动节点作为信标节点。接收方不需要与发送方（信标节点）时间同步。通过利用 TDOA 技术就能准确的定位节点（Luo 等，2006 年）。

（7）利用一组传感器的早期位置信息和统计模型来估计节点的位置。有时候，传感器的位置可以在其布置之前得到。然而，传感器可能无法被部署在预计的位置，但是它可以与其邻居节点联系并依靠概率方式估计自身的位置（Fang 等，2005 年）。

### 18.2.2　WirelessHART 位置测定应用

本节介绍一种基于 WirelessHART 网络的位置感知应用（Zhu 等，2009 年）。

这种应用是完全基于软件的，并且不需要改变 WirelessHART 现场设备。因此，它适用于所有的 WirelessHART 网络。移动用户定位背后的关键想法是以下两种技术：第一种技术是双向比较接收信号强度；另一种技术是利用事先收集的数据来训练电波传播模型以确定最佳参数。在这种方法中，第一步是选取一个电波传播模型，并收集足够的训练数据来训练该模型。然后，在定位过程中，移动用户（如手持设备或电子标签）和现场设备都向网络管理器发送邻居健康报告。这些邻居健康报告同时包含了设备的 ID 信息和接收信号强度等级。随着工人在工厂内走动，工人手持的移动设备将会检测到其周围的现场设备。同样，现场设备也将能够探测到工人的存在。工人附近时常会有三个以上的现场设备。因为现场设备和工人手持的移动设备都向网络管理器发送信息，所以网络管理器反过来可以利用这些信息筛选出不可信的接收信号强度指示（RSSI）。最简单的方法是比较现场设备与手持设备提交的邻居健康报告。如果两者相匹配，那么它们都可以用于测距。如果两者的差值大于某一阈值，那么这对报告将不予考虑。因为网络管理器知道所有现场设备的部署，所以通过利用训练好的定位模型，网络管理器能很容易地、准确地对节点进行定位。

虽然 WirelessHART 在应用层定义了许多种服务，但是它目前并没有规定如何提供位置感知服务。这样就无法通过发布 WirelessHART 协议定义的标准命令来定位设备或工人。尽管可以为设备提供特定的硬件和相关的命令，但是在我们的解决方案中，我们选择不增加额外的硬件负担。对此，我们能依靠的唯一距离参数是物理层提供的接收信号强度。

从理论上说，一个手持设备或者标识卡完全可以通过三角测量法来确定出自己的位置。这是因为通常情况下，工厂中安装了很多现场设备，所以手持设备可以感知到很多自己周围的设备。然而这种解决方案在 WirelessHART 网络中会遇到很多问题。首先从安全角度考虑，WirelessHART 网络中的两个设备不能随意地直接通信。所以即使手持设备可以通过感知从一个现场设备得到的信号强度从而计算出它们之间的距离，但是手持设备并不能直接查询该现场设备的位置信息。当然，手持设备可以向网络管理器查询现场设备的位置信息。然而就像我们先前提到的，WirelessHART 标准还没有定义任何与位置信息相关的命令。而且，我们并不希望我们的解决方案需要对已经安装的设备做任何修改。其次，手持设备可能会收到多于 3 个的距离指示。这些冗余的信息并不能总是帮助提高定位的精确性，相反某些时候甚至会造成混乱。这是因为手持设备或者标识卡并不知道哪些距离指示是精确的。手持设备需要过滤掉错误的距离指示，并从一个候选名单中选择合适的邻居设备来进行定位计算。我们提出的解决方案描述如下。

（1）为了提高定位精度，我们需要获得电波传播模型的准确参数。我们提出的方法首先对当前的环境进行现场调查来收集足够的训练数据；然后，基于这些训

练数据，使用最小二乘法来计算出模型中的最佳参数。

(2) WirelesHART标准要求每个设备（包括手持设备）周期性地向自己的邻居设备发出Keep-Alive报文（时间间隔的默认值30s，也可以由网络管理器根据需要进行配置），同时接收方会发回一个确认报文。通过这种双向通信，每对设备都可以接收到对方的信号强度。

(3) 手持设备或标识卡的定位是在网络管理器中实现的。由于每个WirelessHART设备都会周期性地向网络管理器发送自己的邻居健康报告（时间间隔的默认值30s，也可以由网络管理器根据需要进行配置），网络管理器可以收集足够的信息来支持对手持设备的定位。事实上，网络管理器还可以主动地要求某个指定的设备向自己发送邻居健康报告。如前所述，冗余的信息会对网络管理器造成混淆。但是，本方案中的冗余信息不会对网络管理器造成混淆。这是因为现场设备和手持设备都可以独立地向网络管理器报告信号强度信息。网络管理器对这两者发过来的报告进行匹配。如果两个信号强度值之间的差异大于一个给定的阈值，网络管理器就将丢弃这两个报告。否则，网络管理器将把这两个值的平均值输入到已经训练好的电波传播模型中，从而过滤掉由随机噪声引起的一些不精确的距离指示。

## 18.3 信息物理系统和WirelessHART系统

在从蒸汽机到互联网的工业化过程中，无线技术应用于过程自动化是一个重大的进步。甚至，我们已经开始看到了科技进步的新时代曙光，这种科技进步将深刻地改变社会。互联网的成功是建立在其能在全球范围内传播和整合信息。互联网将各种信息服务进行融合，从而能为用户提供新的和更强大的服务。将来，这些被融合的服务将不仅包括信息服务，还包括先进过程控制技术所需的物理服务。远程医疗的出现就是一个这样的例子。远程医疗包括远程手术，即外科医生将可以对远在他处的患者进行外科手术。另一个例子是远程家庭援助，即智能触觉设备将被远程操作从而为老年人和体弱者分担家务。在未来的智能公路系统中，当遇到危险情况时，配备有自动驾驶助理的汽车将能够调节驾驶员的行为从而避免事故。信息物理系统（Cyber-Physical System，CPS）重点关注的是由于信息和物理控制技术的集成从而能提供的新的技术和服务。信息物理系统是一种物理和工程系统，其操作由一个计算和通信核心进行监控、协调、控制和集成（Stankovic等人，2005）。

无线过程自动化系统是信息物理系统中一个必不可少的组成部分。因为WirelessHART标准是一种能够实现控制应用的技术，所以WirelessHART标准非常适合用来实现许多信息物理系统。与商业应用不同，控制应用对确定性响应、耐受嘈杂环境的能力、防范蓄意攻击的安全机制等都有着更为严格的要求。实时控制系统的响应时间必须被设计成可精确预测的，而这对于一些非确定性的协议（如Wi-Fi

和蓝牙）来说通常是无法保证的。因为 WirelessHART 标准已被设计成可以运行于嘈杂的环境，例如运行在重型机械工厂中，所以它能有效地防范通信信道中的数据丢失。WirelessHART 标准也被设计成能承受某些类型的蓄意攻击。然而，信息物理系统与传统的信息系统（Information Systems，IS）以及物理控制系统（Physical Control Systems，PCS）都有所不同。信息物理系统包含有信息系统和物理控制系统间的交互，而传统的信息系统或物理控制系统都不存在有这种交互。因此，信息物理系统的发展带来了一些新的挑战。在计算方面，信息物理系统带来了一种新的故障模式。然而，传统控制系统或信息处理系统的设计者则不需要考虑这种故障模式。如果一个攻击者了解了信息系统和物理控制系统间的交互，那么他就可能会利用这种新的故障模式来引起重大的系统混乱。特别是当无线技术作为通信和控制的基础设施时，攻击者可能会利用不可预见的缺口制造出非常规的攻击。新的模式和技术必须被开发出来以防范这类攻击。接下来，我们将简要地调研无线技术（如 WirelessHART 标准）布置在过程自动化工厂时带来的安全问题。通过这样做，我们希望能提升学术界和工业界的研发人员对信息安全的意识。

我们可以认为攻击的战略是扰乱物理状态信息流与信息物理系统的命令和控制信息流间的协调。例如，在未来的智能电网中，发电机相位的可靠测量对于电网的安全和有效控制是至关重要的。智能电网的攻击者可能会将其自身插入到控制网络的信息流基础设施中，从而能够造成巨大破坏。这种情况是可以做到的。例如，在控制网络中多个不同地方和在关键时刻干扰无线控制信号。或更糟的是，如果攻击者成功地扮演了某发射机的身份，那么该攻击者就可以对智能电网进行拜占庭（Byzantine）攻击（拜占庭攻击是一种信息战攻击。在拜占庭攻击中，攻击者可能会接管通信网络中的一些控制计算机，然后伪装成健康的计算机给其他计算机发送误导性的信息）。如果不采取相应的针对性措施，错误的相位测量可能会对系统造成严重的损害。虽然许多重要的方法在各种文献中被提出用以防御拜占庭攻击，但是所有的解决方案都必须依赖于一种假设，即网络中所有的节点没有同时受到损害并且至少有一部分节点（在某一下限以上）必须能正确工作以抵御攻击。因此，对于共模模式的攻击，还没有一种有效的防御策略。在共模模式攻击中，攻击者可以利用一个共同的弱点来对所有的节点同时进行攻击并使所用的网络控制部件不能正常工作。这种情况是有可能发生的，例如，一个恶意的控制软件可以被下载到系统的每个节点中并等待被攻击者同时激活。这种类型的攻击在理论上可以克服所有已知的对拜占庭式攻击的防御。

另一方面，信息物理系统具有一些共同的特点。这些特点有助于对信息攻击进行防御。这些特点包括如下内容。

（1）物理系统在控制之下的动态特性是由物理学准则决定的，这一点是任何攻击者都无法改变的。

（2）过程控制下的物理状态变量的变化率可能会比控制系统中的信息流的变化率慢，这种情况通常存在于机械和化工系统中。

（3）信息物理系统的信息价值通常是时间的函数，其价值随着时间的推移可能会大幅降低。

特点（1）的含义是：防御者的信息源本身不会被网络攻击颠覆，尽管这些信息可能在传输和使用的过程中被修改。如果能够直接对过程测量中得到的信息进行安全检查，那么这些检查就不会被攻击者颠覆并可以作为系统安全计算平台的基础。

特点（2）的含义是：防御者可以通过测量和实时仿真技术来获得一个近似的，但足够精确的对系统物理状态的全局描述，或至少能够知道在某个给定的时间内系统是否达到了精度上的要求。这样防御者就可以知道当前的系统状态信息是否可信。这类似于已逝的 Flaviu Cristian 博士基于自己定时异步计算模型所提出的系统设计方法（Cristian and Fetzer，1999）。这里要解决的问题是如何才能有效地利用物理状态变化率较慢的特点来增加检测到恶意攻击的概率。我们认为这个问题是可以解决的，除非攻击者可以以同步的方式同时破坏所有物理状态的测量结果。在任何情况下，我们应该都可以基于本地的测量结果以分层的方式在不同的时间尺度上设计检测系统，从而使攻击者很难做到同步攻击。

特点（3）的含义是：攻击者只能在有限的时间内有效使用从物理系统状态中得到的信息。所以我们只需要保护仍然有价值的物理变量信息就可以了。当然在这种情况下，传统的信息保护方法和体系结构设计需要被重新审视。

我们相信一种防御方式是否有效取决于它能否及时地把全局控制信息和本地物理测量结果关联起来，以及取决于能否在攻击者对信息物理系统造成无法估量的破坏之前调整防守策略。在这里我们假设某些实时约束可以通过信息流基础设施本身或者和物理状态测量值之间的相关性来进行检测。和普遍的观点不同，我们不认为在设计安全系统时硬时序约束是脆弱的。我们认为硬时序约束定义了一个系统的完整性。所以，一个硬时序约束无法被满足则意味着违反了系统的完整性，但并不代表系统崩溃了。这种安全系统的设计方式和已逝 Flaviu Cristian 博士的定时异步系统设计理念相似。它的核心是时序同步的错误是可以被检测到的。在信息物理系统中，在本地物理设备上进行的物理测量可以通过例如硬件的方法来进行加强以检测到时序错误。这些时序错误以时间的函数表现为物理过程的意外行为。一个成功的攻击者必须把攻击的时间和物理测量系统协调好来掩盖自己的攻击。在这种情况下，这些时序约束要求对防御方有利，因为它们有助于定义物理过程的正常行为，并和异常的系统行为进行比较。这使我们有望设计出低开销的入侵检测和预防系统来防御新类型的拒绝服务攻击，比如说目前很难防御的过敏攻击（Chung and Mok，2007）。

有效防御的另外一个重要组成部分是假设当某些攻击成功时如何设计对应的恢复机制。系统恢复概念的核心是故障语义。这里的关键是一个系统应该被设计成不仅能在正常情况下工作，而且当故障发生时也能够在绝大多数情况下按照某种特定的方式工作。对信息物理系统而言，传统的故障模式分类并不令人满意，这是因为它在设计时只考虑到了计算机（硬件）系统。而在信息物理系统中，一个好的分类系统需要考虑到系统的被控物理组件和用于控制的计算机及通信模块之间的交互。例如，机械组件通常情况下出现故障的时间是以秒为单位的，这和计算机系统的反应时间（远低于1s）相比大很多。我们可以利用这个优势来定义信息物理系统特定的故障分类。这时我们需要把用于防御行动的时间考虑在内。例如我们可以通过加入一个故障时间的参数来在故障模式分类中增加一个时间维。当然根据应用程序的具体属性，我们也可以在信息物理系统特定的故障模式分类中增加其他维度。举个例子，当一个信号灯发生故障时，我们不需要让所有的车辆停止通行而是把信号灯置于红灯闪烁模式。这样车辆就可以按照预先定义的四方停止标志来通行。这个例子提供了一种概括故障模式语义的方式：故障语义可以定义为发生故障的系统都必须遵循的协议。这些协议可以被形式化为各种各样的在计算机科学，混合系统以及其他工程分支中的技术。它们可以是与应用程序相关的，并且具有时间维度。

任何对信息攻击的防御都不会是完美的。防御的有效性必然是相对于对攻击者可能造成的破坏而言的。在信息物理系统中，攻击对系统造成的破坏可以通过该系统和正常执行情况下系统行为的偏差来进行量化。由于对信息物理系统的有效攻击速度受到该系统一些物理属性上的限制，对这些攻击的防御可以定义和执行应用程序特定的故障语义。这将有助于设计安全系统。

我们相信安全信息物理系统的设计可以受益于以下假设：系统故障可以通过本地的物理测量来检测到并进一步预测相关可能发生的安全攻击。基于这个假设，对安全攻击的防御取决于在设计系统时如何选择一个好的物理故障语义以及对这些故障的及时检测。我们需要的是用于指定物理上的时序要求的设计原则和用于监测这些约束的工具（Woo 和 Mok，2007）。这些检测设施需要被加入到任何信息物理系统的安全计算基础平台上。

安全问题只有通过过程控制协议的设计者、实现者和最终用户之间的紧密合作来实现。为此，学术界和工业界已经做了大量的研究工作，并通过严格的测试和先进的设计理念来加强 WirelessHART 网络对蓄意信息攻击的保护（Song 等，2008）。然而，我们还需要完成以下一些工作。

1）学术界和工业界应相互合作来了解和运用领域内的知识在传感器上直接进行安全检查以构建对网络攻击的第一条防线。

2）创建一个信息系统架构来利用公用工程系统中信息系统和物理控制系统双

方的过程和时间信息，包括实时仿真设施。

3）设计特定领域的实时数据库服务，以抵御网络攻击，特别是拒绝服务攻击。

4）定量地了解及时检测的成本和设备可以承受的损害之间的权衡。这种损害是一个检测时间和执行反制措施时间的函数。

5）探索适当的故障语义以最大限度地减少损害以及缩短恢复时间。

6）攻击者只能在一个有限的时间内在自己得到的数据失效之前和网络进行同步，并执行攻击，利用这一限制可以探索各种信息保护的方法和架构。例如设计轻量的加密技术来保证对所有新数据的短期保护。

7）了解和利用无线协议和过程控制技术的技术特点，以便实施以上 6 点。

## 18.4　WirelessHART 标准的下一步演进

在制造和自动化环境中，无线技术能做的所有伟大事情都是很容易预测的。但是，我们不会这样做。20 多年前从 HART 标准首次发布开始，HART 标准即开始了其一系列不断的演进。现实情况是，WirelessHART 标准仅仅是 HART 标准演进中的一个延续。HART 标准的设计初衷就是让供应商和最终用户一起解决工厂实际应用的真正需求。在 HART 标准不断演进的过程中，设备基础设施已发展到允许设备满足更大范围内的需求。因此，真正的问题是，“什么是商业驱动以及如何发展设备基础设施以支持这些商业驱动?” 由此，我们可以很容易地预测未来的完善方向。我们首先简要讨论商业方向，然后讨论这些商业方向中涉及的设备及技术。最后，一些有可能被标准化的特定领域也将会被讨论到。

首先看看第一个问题，即“什么是商业驱动?”，所有的经营业绩都是基于资产所产生出来的价值。这些资产覆盖的范围包括人、材料、知识内容、物理性质。商业系统正促使工厂变得更加集成化，工厂操作的要求更加严格。这些工厂也被预计能根据条件和订单的变化实时调整生产进度，并且更加规范。这些目标的实现需要对工业过程有更全面的理解，需要提高对工厂设备状态的理解，还需要更好的数据分析技术。这些工厂的操作人员可能会拥有学位，并且许多是高等学位。这就引申出了第二个问题，“如何发展设备基础设施以支持这些商业驱动?”

针对第二个问题的答案必须考虑几个方面。对过程工业更全面、更深入的监测包括：增加测量、要求测量设备提供更多的诊断信息、提供设备所属过程工业的诊断信息以及实现过去需要手工完成的上线过程。WirelessHART 标准的第一个版本经历了很长的路才使先进测量和诊断成为可能，也能实现过去很难实现的测量。许多工厂基础设施装备不足，以致无法报告先进的诊断信息。无线技术允许这些测量信息能在另种替代的基础设施上传输。在其他情况中，对某些类型的设备（如旋

转设备）的测量是难以进行的。如果将无线设备附加到这类设备上并让无线基础设施负责通信，这样就会使得这类设备的测量容易得多。在其他一些情况中，手工测量是最先进的，无线技术能物有所值的定期获取这些测量并将它们传送出去。这样的一个例子是设备的健康监测。新的无线设备正被集成到传感器中，用以测量振动信息和获取诊断信息，并将这些振动和诊断信息返回给在线中央控制系统。

新设备通常具有先进诊断功能。这些诊断功能可以诊断出设备的健康状况，并在许多情况下可以诊断出与该设备相连的工业过程的健康状况。这些最新的设备通常还具有其他一些先进诊断功能，如可以检测出插线、燃烧器火焰的不稳定、搅拌损失、湿气体、孔板磨损、泄漏和空洞形成。这些新设备能告诉用户它们运行得如何，以及什么时候需要用户进行维护。

为了获得这些智能设备的好处，应用和控制系统需要有很好的集成。为了促进这种集成，HART 7.0 版本采纳了一些新功能，如测量值状态、时间戳、事件锁存和确认、块数据传输，以及完整的 WirelessHART 通信系统。WirelessHART 通信系统能对自身进行调整以满足控制系统的控制和通信要求。更好的集成能导致更少的错误、更好的控制过程、并显著地减少停机时间。

许多新设备具有多个测量值，例如某个液位测量设备可能既包括一个液位测量值，又包括用以指示高液位和低液位的离散值。新的离散规范支持这类混合测量设备。其他一些新设备可能可以提供资产跟踪的功能。位置测量和定位技术被用以解决资产跟踪的应用要求。

WirelessHART 标准的第一个版本包含了无线手持设备。无线手持设备能支持工厂工人直接访问现场设备和装置。无线手持设备在 WirelessHART 标准的后续版本中将会得到进一步加强。WirelessHART 标准中的许多技术都将会得到继续发展。例如，新的无线电技术将会被发布，新的无线电频段也将会被使用。WirelessHART 标准不会仅锁定于 IEEE 802.15.4 标准描述的 16 个信道——WirelessHART 标准可以支持多达 64 个信道。当新的无线技术问世时，WirelessHART 标准的物理层在未来也可以很容易地被替换。

WirelessHART 标准中另一个可能会继续发展的领域是设备的预配置。在某些情况下，对设备的无线预配置将会是很有优势的。WirelessHART 标准的原始版本考虑到了这个问题，并且为公共密钥加密技术敞开了大门。公共密钥加密技术将会被添加到 WirelessHART 标准的后续版本中。

因此，如何通过无线技术实现控制？事实是，早期采用者已经对无线控制进行了努力的测试。这些测试结果已经证明，无线控制系统也能获得良好的控制性能。随着无线网络调度技术的完善以及更好电池技术的出现，无线控制将会被应用到越来越多的工业现场。

### 18.4.1 离散设备和离散值

在过程工业的大多数工厂中，离散测量和动作在整个工厂控制系统和操作中发挥着重要的作用。在一些工厂区域，控制系统中输入输出总量的 80% 以上可能是离散的。传统上，这些离散的要求已经通过在控制系统中使用离散输入输出卡，或者通过 PLC 的接口连接到过程控制系统而得以解决。通常，这些离散设备或者是已存在的测量设备的一部分，或者是用来支持这些测量设备。例如，液位和压力仪器通常包括相关的限位开关和一些诊断信息。这些诊断信息最好作为离散量被传输。

离散值可表示为简单离散值，或表示为更复杂的状态信息。在包括限位开关和开/关设备的离散案例中，离散值的值是简单的 1 或 0。在更复杂的离散案例中，状态信息要求多个量值，例如阀门的状态量有开、关、正在打开、或正在关闭。

在简单的开/关型案例中，量值可以作为离散值块或数据位被传送。单个状态可以涉及一定范围的量值。在更多的情况下，开/关阀门或其他设备的状态量值应该伴随着它的状态信息和时间戳一起被传送。

包括离散值和状态信息在内的全面扩张代表着 HART 标准的不断演进，因为它满足了更多的测量要求以及工业现场中更广泛的需求。

### 18.4.2 定位

定位技术可用于跟踪工厂车间中的人员和资产。工厂车间中的人员跟踪对于人身安全而言是至关重要的，因为工厂车间中常存在有高危险的有毒或易燃化学品。资产跟踪使车间人员能更容易地找到材料和设备。最初的 WirelessHART 标准已经包含了许多定位应用所需的功能。例如所有设备对时间都有同样的时间概念、必须能够发送通告报文、路由报文、跟踪信号强度、发布健康报告和利用代理设备的设备地址来路由报文。随着第一版 WirelessHART 标准的发布，离线定位计算是有可能实现的。现在缺少的是一种针对现场设备的标准化方式，以便为控制室或手持设备上运行的定位应用程序提供定位信息。

为了满足这些需求，定位跟踪设备与定位应用程序间交互的命令将会被标准化，并被添加到 WirelessHART 标准的未来版本中。这些命令将使得在工厂车间内定位资产设备成为可能。WirelessHART 标准的另一种增强将会是添加允许跟踪设备与定位应用程序间通信的会话。这些通信的内容将会被完全地加密和保护。

### 18.4.3 手持设备

WirelessHART 手持设备被用于设备的安装和维护，也被用于上位机上的定位应用。在任何情况下，WirelessHART 手持设备只有通过网络管理器的认证后才可以加入 WirelessHART 网络。通过认证后，手持设备和网络设备之间的通信都必须

是安全的。

在WirelessHART标准初始版本的制定过程中，相当多的讨论都围绕着如何限制无线手持设备的通信。WirelessHART手持设备被限制为只能和与其相连的WirelessHART网络设备建立会话、路由、超帧和链路。这样，WirelessHART手持设备的所有通信都会被限制在与其相连的WirelessHART网络设备之间。

作为定位跟踪应用的一部分，WirelessHART手持设备的应用范围有必要进行扩展。出于定位应用的目的，使用手持设备来定位资产以及与控制室操作人员通信都会成为必要的。在这些情况下，一种特别的会话将会被建立起来，用以允许报文在手持设备、控制室、定位应用程序之间安全地交互。

### 18.4.4 手持式的公共/私有密钥

在WirelessHART标准的最初版本中，一系列安全机制被用以确保设备直到通过身份认证后才能加入网络。一旦通过身份认证后，所有的通信都是私有的。其中一种安全机制是无线预配置。无线预配置之前被讨论过，但是在WirelessHART标准中并没有被指定说明。为了允许这种能力，WirelessHART标准的最初版本预留了一定的地方以便指明和利用额外的安全机制。

展望以后，一种即将被添加的安全功能是公共密钥加密。公共密钥加密技术有几种。其中，被认为最有前途的一种是椭圆曲线Diffie-Hellman（ECDH）算法。在接受这些公共密钥加密技术之前，了解这些技术以及这些技术实现所需的资源（内存和CPU）是很重要的。更多的工作正在进行中。

### 18.4.5 无线控制

利用无线作为闭环控制的基础设施，这对设备制造商提出了许多技术挑战。大多数多回路控制器的频率是测量采样频率的2～10倍。此外，为了最大限度地减少控制的变化，典型的经验法则是：反馈控制的执行速度应该比过程响应时间（过程时间常量加上过程延迟）快4～10倍。对于无线系统而言，电池寿命是至关重要的。因此，无线系统的设计目标是尽可能地减少数据通信，然而这对于可靠传输似乎又是一个巨大的障碍。

WirelessHART标准所采取的方法是允许设备在必要的时候才采样数据，在采样值变化时才发送数据。这种方法的使用显著地减少了网络上的通信开销。在实际工业现场中，这种技术的使用可使无线通信量减少到原来的1/10～1/30。那么系统的控制性能方面会受到怎样的影响呢？

当测量不能定期更新时，为了提供最好的控制，PID可能需要进行重组，以体现从最后一次更新开始对所期望的过程响应的复位贡献。第16.2节已经阐述了我们在这个方面的研究工作。

# 第 19 章　WirelessHART 案例分析

## 19.1　项目介绍

某财富 500 强公司已经拥有一系列有线 HART 设备，希望在此基础上开发无线 HART 产品。通过了解和比较市场上的 WirelessHART 协议栈提供商，他们寻求到 AwiaTech 公司。AwiaTech 是一家总部在美国得克萨斯州奥斯丁市的专注于 WirelessHART 协议栈及网络管理器软件的高科技公司，拥有全球领先的 WirelessHART，及高可靠性网络技术。经 AwiaTech 许可，我们得以使用此经典案例。在此，作者表示感谢。

## 19.2　案例分析

目前市场上的 WirelessHART 的适配器都是针对于使用 FSK 的有线 HART 设备。本案例中客户公司的有线 HART 设备使用 RS-232 作为有线的接口，无法使用现有的 WirelessHART 适配器，因此希望同 AwiaTech 合作开发。

## 19.3　AwiaTech 解决方案合作开发路线图

1. 前期调研会议：确定客户的需要并明确定义项目的范围和期望。

2. 模型演示：根据 AwiaTech 现有技术快速建立一个基于客户设备的 WirelessHART 模型。

3. 方案：一旦确定了用户的需求，AwiaTech 提供详细的建议，其中包含解决方案，并定义项目的可交付结果。

4. 实施：进入项目实施阶段。

1）开始：明确客户需求，资源安排等。

2）过程：开发时间表和里程碑，以及每个里程碑的交付内容。

3）沟通：定期同客户沟通，让客户及时了解项目进展速度。

5. 提供培训：项目范围和定义的产品解决方案、培训。

6. 测试：对产品进行测试以确认满足所有注册及验收要求。

7. 注册：提交最终产品进行注册和验收。

## 19.4 客户需求理解

通过双方的详细讨论，客户表达了对产品质量，完成时间（Time-To-Market），节省开发成本的高要求。

1. 客户只需要能适合于客户的三款现有 HART 产品线的 WirelessHART 模块。

2. 客户只需要一个 WirelessHART 模块连接到一个客户设备。

3. 设备反应速度足够快，无需延迟应答机制（DRM）。

4. 客户现有的设备是基于有线 HART 版本 5。WirelessHART 只有版本 7 以上才支持。客户希望对已有设备内的硬件软件不需要做任何的修改。

## 19.5 方案比较

基于以上的客户分析，AwiaTech 提供两套开发方案。

1. 基于 RS-232-HART 设备的通用 WirelessHART 适配器。

优点：

1）此适配器适用于任何基于 RS-232 的 HART 设备。

2）此适配器在同一时间与多个基于 RS-232 HART 的设备工作。

3）支持延迟应答机制 DRM。

缺点：

1）有相当部分功能客户并不需要。作为定制开发，这会大幅增加客户的时间和成本。

2. 客户专用的 WirelessHART 轻型适配器（Adapter Lite）。

优点：

1）可以附加，并捆绑到客户的所有现有 HART 设备。

2）支持客户设备所支持的所有标准命令。

3）支持版本 5 和版本 7 之间的命令转换。

4）支持所有特定于设备的命令。

5）在上电后将从设备读取某些命令并进行缓存。对大多数其他命令轻型适配器只是在 GW/NM 和客户设备之间传递。

6）将支持猝发模式，客户设备目前不支持猝发模式。

7）快速开发，快速进入市场，满足客户技术要求。

缺点：

1）同一时间只限于与一台 RS-232 HART 设备工作。

2）缺乏 DRM 等性能。

## 19.6　方案实施

客户最终决定使用轻型适配器方案。最终项目分两个阶段实施：

原型交付——一个月。

1）实现客户 RS-232 设备支持的所有通用和常用命令的子集。

2）实现设备特定的读取命令包括索引的命令。

实现最终产品，完成测试，交付——两个月。

## 19.7　AwiaTech WirelessHART 模块详解

### 19.7.1　系统架构

AwiaNet 提供了一个在主机应用和传感器之间传递数据的无线通道。从图 19-1 中可以看到，AwiaNet 提供两个接口，一个是 AwiaNet 和传感器之间的接口，另一个是 AwiaNet 和主机应用之间的接口。

通常意义下的网关（Gateway）在一个 WirelessHART 网络中分成 3 个部分：1）接入点（Access point），用于提供跟网络的无线通信；2）网关（GW），用于提供到主机应用程序的接口；3）网络管理器（Network Manager），用于管理整个无线网络。在 AwiaNet 中，接入点是一个跟 PC 连接的硬件模块，我们称为 Awia Captain；而网关和网络管理器则是以软件形式存在，称为 Awia Vanguard（AwiaNet 天卫）。网络节点（又称设备节点）则称为 Awia Warrior（Awia 天兵），它们组成 AwiaNet 的其余部分。

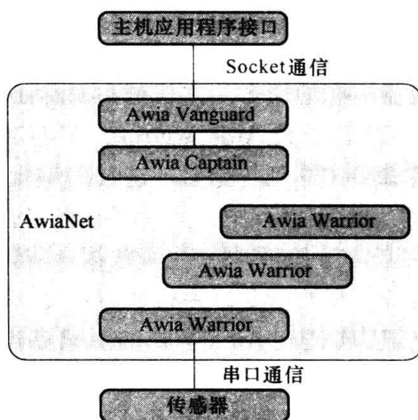



图 19-1　AwiaNet 网络示意图

AwiaTech WirelessHART 评估套件是一个包含了组成一个完整的 AwiaNet 的基本组件的演示系统（见图 19-1），其中还包含一个主控应用程序的演示版。同时，在其中的网络节点（Awia Warrior）中还内置了一个模拟的传感器，可在演示系统中被激活以用于测试。

AwiaTech WirelessHART 评估套件同时也为主控应用程序开发者和传感器开发者提供了相应的接口。

### 19.7.2 主机应用程序接口

用户可以利用主机应用程序接口（Host API）开发自己的主控应用程序。AwiaTech WirelessHART 评估套件中提供的演示版主控应用程序是用 Java 开发的，但用户可以选择任意的开发语言进行开发，因为跟网关的通信是基于标准的 Socket 接口。网关和主机应用程序以命令的形式交互消息，具体的通信协议请参见 AwiaTech 用户手册。

下面描述如何设置主机应用以从设备节点获取猝发数据。

1）首先，主机应用建立跟网关的 socket 连接。

2）主机应用周期性地调用读取命令以发现新加入网络的传感器。

3）一旦收到反馈信息，主机应用就调用订阅命令去启动传感器发布数据。传感器就会周期性地将数据发送到网关的缓存区，这些数据将被转发到主机应用。

### 19.7.3 设备端应用程序接口

如图 19-1 所示，一个传感器可以通过串口（COM 口或基于 USB 的虚拟 COM 口）跟 Awia Warrior 设备节点以命令的形式进行通信。具体的通信协议请参见 AwiaTech 用户手册。

下面是几个常用的命令。命令数据的最大长度是 72B，也可以是 0。

1. 从 Awia Warrior 设备节点到传感器：主机数据—猝发模式（命令 170）

这是一个 AwiaTech 设备特有的命令。主机通过命令 170 发送这个字节序列到网关。同时，网关将命令 170 转送到 Awia Warrior。只有当从网关收到了命令 170 后，Awia Warrior 才会发送命令 170 到传感器。这时，Awia Warrior 首先将命令数据复制到为命令 170 设置的本地数据缓存中，然后同时将它们发送到传感器。

2. 从 Awia Warrior 设备节点到传感器：主机数据—非猝发模式（命令 171）

这是一个 AwiaTech 设备特有的命令，主机通过命令 171 发送这个字节序列到网关。同时，网关将命令 171 转送到 Awia Warrior。只有当从网关收到了命令 171 后，Awia Warrior 才会发送命令 171 到传感器。这时，Awia Warrior 直接将命令数据发送给传感器，而无需将命令数据复制到为命令 171 设置的本地数据缓存中。

3. 从传感器到 Awia Warrior 设备节点：传感器数据—猝发模式（命令 170）

这是一个 AwiaTech 设备特有的命令。传感器通过这个命令 170 发送一系列字节用于猝发。然后 Awia Warrior 将这些字节复制到为命令 170 设置的本地数据缓存中。如果主机通过命令 170 订购了发布数据，那么 Awia Warrior 将周期性地通过猝发命令 170 将缓存中的数据发送到网关。

4. 从传感器到 Awia Warrior 设备节点：传感器数据—非猝发模式（命令 171）

这是一个 AwiaTech 设备特有的命令。传感器通过这个命令 171 发送一系列字节。然后 Awia Warrior 将这些字节复制到为命令 171 设置的本地数据缓存中。主机通过给 Awia Warrior 发送命令 171 来获取在缓存中的数据。

5. 从传感器到 Awia Warrior 设备节点：设置网络 ID（命令 773）

这是一个标准的 WirelessHART 命令。这个命令用于设置 Awia Warrior 应该加入的网络的网络 ID。这样，Awia Warrior 设备节点从上电开始就去捕捉从具有该网络 ID 的网络发出的广播信息以加入网络。

6. 从传感器到 Awia Warrior 设备节点：W 写 Join Key（命令 961）

这是一个标准的 WirelessHART 命令。这个命令用来设置设备的 Join key。在网络加入过程中，Join key 用来对信息加密。

### 19.7.4 Awia Net 的应用方式

1. 将 AwiaNet 用作数据传输媒介—猝发模式

跟其他的网络设施一样，AwiaNet 可以作为实现两点间进行数据交换的媒介。在这里，交换数据的两点是主机应用程序和现场的传感器。为了实现这个目标，AwiaNet 从主机应用接收数据，然后传递到传感器，或者是反向的操作。

1）从主机到传感器：主机应用程序调用命令 170，并带一个字节串作为参数发送到传感器。AwiaNet 将数据路由到跟传感器相连的 Awia Warrior，并将数据复制到 Awia Warrior 中为命令 170 设置的缓存中，然后向传感器发送命令 170，并带上相同的字节串作为参数。

2）从传感器到主机：传感器发送命令 170 到 Awia Warrior，也以一个字节串作为参数。Awia Warrior 将缓存字节串。如果主机已启动了猝发模式，则 Awia Warrior 将周期性地将缓存中的数据发布给网关。在收到 Awia Warrior 的数据更新时，网关将数据放入其缓存，并将数据转发给主机应用。有时，主机应用也可以发命令读取网关缓存中的字节串数据。

主机应用和传感器之间的通信协议，即两者之间交换的字节串的语义，由用户自己定义。主机应用和传感器需要管理通信的确认和重传，因为在无线网络中存在信息丢失的可能。另外，因为每个包最多只能传递 72B 的数据，对于超过 72B 的数据，需要在发送端进行数据的分割，在接收端进行数据的组装。

2. 将 AwiaNet 用作数据传输媒介—非猝发模式

命令 170 主要用于以基于订购的方式获取传感器的数据。它非常适用于传感器数据频繁更新的场合，这样主机应用不必每次都要主动去触发数据更新。然而，在很多其他的应用场合，主机应用只需要隔很长时间读取一次传感器数据即可，或者只是偶尔读一下数据，这时，采用被动数据获取方式会更好一些。主机应用没有必要为数据更新进行订购。AwiaNet 通过命令 171 支持这种工作方式。

1）从主机到传感器：主机应用发出命令 171 和一个要发送到传感器的字节串。AwiaNet 将数据路由到跟传感器相连的 Awia Warrior，而 Awia Warrior 将同样的字节串跟命令 171 一起发送到传感器。

2）从传感器到主机：传感器将命令 171 和一个字节串一起发送到 Awia Warrior。Awia Warrior 将数据复制到为命令 171 设置的本地缓存中。独立于此，当 Awia Warrior 收到从网关发送的命令 171，它将用其缓存中的数据为命令 171 准备响应消息，并发送回网关。网关没有为命令 171 设置的缓存，而是直接把数据转发给主机。

跟基于订购的方法相同，主机应用和传感器之间的通信协议由用户自己定义。

3. 在一个 WirelessHART 设备中使用 Awia Warrior

Awia Warrior 可以作为一个独立的 WirelessHART 设备。一般来说，一个 WirelessHART 设备在部署前需要进行设置。设置步骤包括一般的操作和安全方面的考虑。Awia Warrior 被设计成需要最少的配置。对一般操作来说，只需要两个参数：第一，是 WirelessHART 设备想要加入的网络的网络 ID；第二，是加入密钥。用户可以通过串口通信来设置 Awia Warrior 的网络 ID 和加入密钥。或者，用户也可以用评估套件使用的网络 ID 和加入密钥来设置被加入的网络。通过这些信息，一个配备了 Awia Warrior 的设备可以上电后自动加入 WirelessHART 网络。

4. 将 AwiaNet 用作 WirelessHART 的评估工具

AwiaTech WirelessHART 评估套件的一个主要的目的就是让用户来体验和学习 WirelessHART。利用评估套件中包含的软硬件部件，可以很快地搭建一个如前所述的 WirelessHART 网络。用户也可以一起使用 HART 通信基金会提供的 WiAnalys 工具来观测 WirelessHART 网络的通信。

# 第 20 章　属性和域值

## 20.1　报文中字段值的注解

网络管理器可以设置大部分的设备属性值。这里，我们列出了一些设备属性值的默认值，即网络管理器没有配置时的初始值（见表 20-1）。

**表 20-1　时间相关的参数**

| 属　　性 | 含　　义 | 默　认　值 |
| --- | --- | --- |
| ActiveSearchShedTime | 设备在加入网络时处于主动搜索模式的最大时间。该时间段失效后，设备将转换到被动搜索模式 | 4000s |
| advertiseInterval | 用于发送通告 DLPDU 报文的时间间隔 | 无。在网络形成阶段需要尽可能快地发送通告报文 |
| AdWaitTimeout | 试图接收额外通告报文的等待时间 | 30s |
| BcastReplyTime | 回复广播报文的最长等待时间 | 60s |
| ChannelSearchTime | 停留在某个给定信道上侦听通告报文的时间 | 400ms |
| DefaultTTL | 数据报的生存跳数，用于规定报文在被丢弃前能被转发的次数 | 32 |
| discoveryInterval | 用以规定在发现链路上随机发送 Keep-Alive 报文的时间间隔 | 无 |
| HealthReportTime | 发送健康报告的时间间隔 | 15min |
| JoinRspTimeout | 响应入网请求的超时时间 | keepAliveInterval |
| keepAliveInterval | 设备必须与每个相邻设备成功通信的间隔时间。设备在收到邻居设备发送过来的报文后，将复位该邻居设备对应的 Keep-Alive 定时器 | 30s |
| maxJoinRetries | 入网重试次数 | 5 |
| maxReplyTime | 传输层用来触发重传的最长等待时间 | 30s |
| maxPacketAge | 报文在网络中存活的最大时隙数 | 300s |
| maxRetries | 传输层在发送响应报文时的重传次数 | 5 |

（续）

| 属　性 | 含　义 | 默认值 |
|---|---|---|
| minAdsNeeded | 在发出入网请求前，设备被允许接收不同通告报文的数量 | 3 |
| PassiveCycleTime | 当设备处于被动搜索模式时，设备在睡眠和侦听之间的循环周期。设备的睡眠时间等于 PassiveCycleTime 减去 PassiveWakeTime | 600s |
| PassiveWakeTime | 当设备处于被动搜索模式时，设备处于侦听状态的时间 | 6.5s |
| pathFailInterval | 设备与某个邻居设备间没有成功通信的时间间隔。设备在该时间间隔内一直都无法与某个邻居设备成功的通信，则表明该设备与该邻居设备间的路径失效了 | 无 |

## 20.2 WirelessHART 报文字段

WirelessHART 标准的底层采用的是 IEEE 802.15.4 标准。IEEE 802.15.4 报文中的一些字段是固定的，或者对 WirelessHART 报文来说是有限的。此外，某些类型的 WirelessHART 报文不需要 IEEE 802.15.4 报文中的某些字段（见表 20-2 ~ 表 20-9）。

表 20-2　物理层报文格式

| 层 | 名　称 | 字节数 | 备注说明 |
|---|---|---|---|
| 物理层 | 前同步码 | 4 | 与 IEEE 802.15.4 标准一致 |
| | 定界符 | 1 | 与 IEEE 802.15.4 标准一致 |
| | 字节计数器 | 1 | 与 IEEE 802.15.4 标准一致 |
| 上层 | 载荷 | * | 与 IEEE 802.15.4 标准一致 |

表 20-3　数据链路层报文格式

| 层 | 名　称 | 字节数 | 备注说明 |
|---|---|---|---|
| 物理层 | 头部 | 6 | 与 IEEE 802.15.4 标准一致 |
| 数据链路层 | 帧控制字段 | 1 | 0x41（与 IEEE 802.15.4 标准一致） |
| | 地址描述符 | 1 | 0x88，0x8C，0xC8 或 0xCC（与 IEEE 802.15.4 标准一致） |
| | 序列号 | 1 | 绝对时隙数的最低有效字节（与 IEEE 802.15.4 标准一致） |
| | 网络号 | 2 | 与 IEEE 802.15.4 标准一致 |

（续）

| 层 | 名　　称 | 字 节 数 | 备 注 说 明 |
|---|---|---|---|
| 数据链路层 | 目标地址 | 2/8 | 与 IEEE 802. 15. 4 标准一致 |
| | 源地址 | 2/8 | 与 IEEE 802. 15. 4 标准一致 |
| | DLPDU 描述符 | 1 | — |
| 上层 | 载荷 | * | — |
| 数据链路层 | MIC | 4 | — |
| | CRC | 2 | 与 IEEE 802. 15. 4 标准一致 |

**表 20-4 数据链路层确认报文格式**

| 层 | 名　　称 | 字 节 数 | 备 注 说 明 |
|---|---|---|---|
| 物理层 | 头部 | 6 | 与 IEEE 802. 15. 4 标准一致 |
| 数据链路层 | 帧控制字段 | 1 | 0x41（与 IEEE 802. 15. 4 标准一致） |
| | 地址描述符 | 1 | 0x88，0x8C，0xC8 或 0xCC（与 IEEE 802. 15. 4 标准一致） |
| | 帧序列号 | 1 | 绝对时隙数的最低有效字节（与 IEEE 802. 15. 4 标准一致） |
| | 网络号 | 2 | 与 IEEE 802. 15. 4 标准一致 |
| | 目标地址 | 2/8 | 与 IEEE 802. 15. 4 标准一致 |
| | 源地址 | 2/8 | 与 IEEE 802. 15. 4 标准一致 |
| | DLPDU 描述符 | 1 | 依赖于接收到的报文 |
| | 状态 | 1 | — |
| | 时间调整 | 2 | — |
| | MIC | 4 | — |
| | CRC | 2 | 与 IEEE 802. 15. 4 标准一致 |

**表 20-5 数据链路层通告报文格式**

| 层 | 名　　称 | 字 节 数 | 备 注 说 明 |
|---|---|---|---|
| 物理层 | 头部 | 6 | 与 IEEE 802. 15. 4 标准一致 |
| 数据链路层 | 帧控制字段 | 1 | 0x41（与 IEEE 802. 15. 4 标准一致） |
| | 地址描述符 | 1 | 0x88（与 IEEE 802. 15. 4 标准一致） |
| | 帧序列号 | 1 | 绝对时隙数的最低有效字节（与 IEEE 802. 15. 4 标准一致） |
| | 网络号 | 2 | 与 IEEE 802. 15. 4 标准一致 |

（续）

| 层 | 名　称 | 字　节　数 | 备注说明 |
|---|---|---|---|
| 数据链路层 | 目标地址 | 2 | 0xFFFF（与 IEEE 802.15.4 标准一致） |
| | 源地址 | 2 | 与 IEEE 802.15.4 标准一致 |
| | DLPDU 描述符 | 1 | 0x31 或 0x11 |
| | 绝对时隙数 | 5 | — |
| | 加入网络控制 | 1 | — |
| | 信道图大小 | 1 | — |
| | 信道图 | * | — |
| | 图路由 ID | 2 | 该设备分配给新设备的图 ID |
| | 超帧号 | 1 | — |
| | 超帧详情 | * | — |
| | MIC | 4 | — |
| | CRC | 2 | 与 IEEE 802.15.4 标准一致 |

**表 20-6　数据链路层 Keep-Alive 报文格式**

| 层 | 名　称 | 字　节　数 | 备注说明 |
|---|---|---|---|
| 物理层 | 头部 | 6 | 与 IEEE 802.15.4 标准一致 |
| 数据链路层 | 帧控制字段 | 1 | 0x41（与 IEEE 802.15.4 标准一致） |
| | 地址描述符 | 1 | 0x88（与 IEEE 802.15.4 标准一致） |
| | 帧序列号 | 1 | 绝对时隙数的最低有效字节（与 IEEE 802.15.4 标准一致） |
| | 网络号 | 2 | 与 IEEE 802.15.4 标准一致 |
| | 目标地址 | 2 | 0xFFFF（与 IEEE 802.15.4 标准一致） |
| | 源地址 | 2/8 | 如果设备地址不是短地址，那么此值为 8（与 IEEE 802.15.4 标准一致） |
| | DLPDU 描述符 | 1 | 0x3A 或者 0x1A。如果新设备的地址不是短地址，那么此值为 0x32 或者 0x12 |
| | MIC | 4 | — |
| | CRC | 2 | 与 IEEE 802.15.4 标准一致与 IEEE 802.15.4 标准一致 |

表 20-7 数据链路层断开连接报文格式

| 层 | 名 称 | 字 节 数 | 备注说明 |
|---|---|---|---|
| 物理层 | 头部 | 6 | 与 IEEE 802.15.4 标准一致 |
| 数据链路层 | 帧控制字段 | 1 | 0x41（与 IEEE 802.15.4 标准一致） |
| | 地址描述符 | 1 | 0x88（与 IEEE 802.15.4 标准一致） |
| | 帧序列号 | 1 | 绝对时隙数的最低有效字节（与 IEEE 802.15.4 标准一致） |
| | 网络号 | 2 | 与 IEEE 802.15.4 标准一致 |
| | 目标地址 | 2 | 0xFFFF（与 IEEE 802.15.4 标准一致） |
| | 源地址 | 2 | 与 IEEE 802.15.4 标准一致 |
| | DLPDU 描述符 | 1 | 0x3B 或 0x1B |
| | MIC | 4 | — |
| | CRC | 2 | 与 IEEE 802.15.4 标准一致 |

表 20-8 网络层报文格式

| 层 | 名 称 | 字 节 数 | 备注说明 |
|---|---|---|---|
| 物理层 | 头部 | 6 | 与 IEEE 802.15.4 标准一致 |
| 数据链路层 | 头部 | * | — |
| 网络层 | 控制字节 | 1 | — |
| | 生存时间 | 1 | — |
| | ASN Snippet | 2 | — |
| | 图路由 ID | 2 | — |
| | 目标地址 | 2/8 | — |
| | 源地址 | 2/8 | — |
| | （可选）代理路由/源路由 | 2/4/6/8/10 | — |
| 网络层/安全 | 安全控制字节 | 1 | — |
| | 计数器 | 1/4 | — |
| | MIC | 4 | — |
| 传输层 | 传输层控制字节 | 1 | 包括序列号 |
| | 设备状态 | 1 | |
| | 扩展设备状态 | 1 | |
| 上层 | 载荷 | * | |
| 数据链路层 | 帧尾 | 6 | |

表 20-9　应用层报文格式

| 层 | 名　称 | 字　节　数 | 备注说明 |
| --- | --- | --- | --- |
| 物理层 | 头部 | 6 | 遵循 IEEE 802.15.4 标准 |
| 数据链路层 | 头部 | * | — |
| 网络层 | 头部 | * | — |
| 应用层 | 命令 | 2 | — |
| | 字节计数 | 1 | — |
| | 数据 | * | 当多个命令时，这三个字段可以重复 |
| 数据链路层 | 帧尾 | 6 | |

# 第21章　符号和缩写

表21-1　符号和缩写

| 名　字 | 定　义 |
|---|---|
| 802.15.4 | IEEE STD 802.15.4-2006 标准的一般表示。当谈到物理层时，它是指在2.4GHz 频段直接序列扩频（DSSS）物理层采用的 OQPSK 调制 |
| ACK | Acknowledge，确认 |
| AE | Application Entity，应用实体 |
| AES | Advanced Encryption Standard，高级加密标准 |
| AL | Application Layer，应用层 |
| AOA | Angle of Arrival，到达角 |
| AP | Application Process，应用进程 |
| API | Application Program Interface，应用程序界面 |
| APDU | Application Protocol Data Unit，应用协议数据单元 |
| APO | Application Object，应用对象 |
| AR | Application Relationship，应用关系 |
| AREP | Application Relationship Endpoint，应用关系端点 |
| ARPM | Application Relationship Protocol Machine，应用关系协议机 |
| ARQ | Automatic Repeat Request，自动重传请求 |
| ASCII | American Standard Code for Information Interchange，美国信息交换标准码 |
| ASE | Application Service Element，应用服务元素 |
| ASN | Absolute Slot Number，绝对时隙数 |
| AWGN | Additive White Gaussian Noise，加性高斯白噪声 |
| BACK | Burst Acknowledge，猝发确认 |
| BER | Bit Error Rate，误码率 |
| CBC-MAC | Cipher Block Chaining Message Authentication Code，密码块链接消息认证码 |
| CCA | Clear Channel Assessment，空闲信道评估 |
| CCM | Counter with CBC-MAC（mode of operation），操作模式下的 CBC-MAC 计数器 |
| CCM* | extension of CCM，扩展 CCM |
| Cnf | Confirmation，证实 |
| COTS | Commercial Off The Shelf，商业现成的 |

（续）

| 名　字 | 定　义 |
|---|---|
| CPS | Cyber-Physical System，信息物理系统 |
| CPU | Central Process Unit，中央处理单元 |
| CRC | Cyclic Redundancy Check，环冗余校验 |
| CSMA | Carrier Sense Multiple Access，载波侦听多路访问 |
| CSMA-CA | CSMA with Collision Avoidance，带冲突避免的载波侦听多路访问 |
| dB | Relative Power Decibels，相对功率分贝 |
| dBi | dBi 以分贝为单位描述天线的增益。字母“i”表示该增益与各向同性天线有关 |
| dBm | dBm 是一个表示功率绝对值的值，也可以认为是以 1mW 功率为基准的一个比值。0dBm = 1mW；10dBm = 10mW；20dBm = 100mW；30dBm = 1W |
| DCS | Distributed Control System，分布式控制系统 |
| DDL | Device Description Language，设备描述语言 |
| DL- | Data-Link Layer（as a prefix），数据链路层（前缀） |
| DLE | DL-Entity（the local active instance of the data-link layer），DL 实体（数据链路层本地的活动实例） |
| DLL | Data-Link Layer，数据链路层 |
| DLM | DL-Management，DL 管理 |
| DLMS | DL-Management Service，DL 管理服务 |
| DLPDU | Data-Link Protocol Data Unit（i.e.，a Data-Link Layer packet），数据链路协议数据单元（即一个数据链路层数据报） |
| DLS | DL-Service，DL 服务 |
| DLSDU | DL-Service-Data-Unit，DL 服务数据单元 |
| DR | Delayed Response，延迟反应 |
| DRM | Delayed Response Mechanism，延迟反应机制 |
| DSN | Data Sequence Number，数据序列号 |
| DSSS | Direct Sequence Spread Spectrum，直接序列扩频 |
| DUT | Device Under Test，被测设备 |
| ECDH | Elliptic Curve Diffie-Hellman，椭圆曲线 Diffie-Hellman |
| EDD | Electronic Device Description，电子设备描述 |
| EDDL | Electronic Device Description Language，电子设备描述语言 |
| EDF | Earliest Deadline First，最早时限优先 |
| EIRP | Effective Isotropic Radiated Power，有效全向辐射功率 |
| ERP | Effective Radiated Power，有效辐射功率 |
| EUI-64 | Extended Unique Identifier（64 bits long），扩展唯一标识符（64 位长） |

（续）

| 名　字 | 定　义 |
| --- | --- |
| FAL | Fieldbus Application Layer，现场总线应用层 |
| FCC | Federal Communications Commission，美国联邦通信委员会 |
| FF | Foundation Fieldbus，美国联邦通信委员会 |
| FFD | Full Function Device，全功能设备 |
| FSK | Frequency Shift Keyed，频移键控 |
| FTA | Field Termination Assembly，现场终端集合 |
| FHSS | Frequency Hopping Spread Spectrum，跳频扩频 |
| FSMP | FAL Service Protocol Machine，FAL 服务协议机 |
| HART | Highway Addressable Remote Transducer，可寻址远程传感器高速通道 |
| HCF | HART Communication Foundation，HART 通信基金会 |
| IAE | Integral Absolute Error，绝对误差积分 |
| ID | Identifier，标识符 |
| IEC | International Electrotechnical Commission，国际电工委员会 |
| IEEE | The Institute of Electrical and Electronics Engineers，电气和电子工程师学会 |
| Ind | Indication，指示 |
| IO | Input Output，输入输出 |
| I/O | Input Output，输入输出 |
| IS | Information System，信息系统 |
| ISO | International Organization for Standardization，国际标准化组织 |
| ISM | Industry，Scientific，Medical frequency bands，工业、科学、医疗频段 |
| ITU-T | International Telecommunication Union-Telecommunication Standardization Sector，国际电信联盟-电信标准化部门 |
| LLC | Logical Link Control，逻辑链路控制 |
| LED | Light Emitting Diode，发光二极管 |
| LoS | Line of Sight，an unobstructed distance between a transmitter and a receiver，视距，发射器和接收器间通畅的距离 |
| LSB | Least Significant Byte. The LSB is always the last byte transmitted over a HART data link，最低有效字节。最低有效字节是 HART 数据链路上被最后传送的字节 |
| MAC | Medium Access Control，介质访问控制 |
| MIC | Message Integrity Code，消息完整性代码 |
| MSB | Most Significant Byte. The MSB is always the first byte transmitted over a HART data link，最高有效字节。最高有效字节是 HART 数据链路上被第一个传送的字节 |
| NL | Network Layer，网络层 |

（续）

| 名　字 | 定　义 |
|---|---|
| NLOS | Non-Line-of-Sight，非视距 |
| NPDU | Network PDU，网络 PDU |
| OLE | Object Linking and Embedding，对象连接与嵌入 |
| OPC | OLE for Process Control，用于过程控制的 OLE |
| OQPSK | Offset Quadrature Phase Shift Keying，偏移正交相移键控 |
| OS | Operating System，操作系统 |
| OSI | Open System Interconnection，开放系统互连 |
| OUI | Organizationally Unique Identifier，组织唯一标识符 |
| PAN | Personal Area Network，个人区域网络 |
| PCP | Priority Ceiling Protocol，优先级上限协议 |
| PCS | Physical Control System，物理控制系统 |
| PER | Packet Error Rate，报文错误率 |
| PDU | Protocol Data Unit. The packet of information being communicated，协议数据单元。被传送的信息包 |
| PhPDU | Physical Layer Protocol Data Unit（i. e.，a Physical Layer packet），物理层协议数据单元（即物理层报文） |
| PHY | Physical Layer，物理层 |
| PIB | PAN Information Base，个人区域网络信息库 |
| PID | Proportional，Integral and Derivative，比例，积分和微分 |
| PLC | Programmable Logic Controller，可编程逻辑控制器 |
| PPDU | PhPDU |
| ppm | parts per million，百万分率 |
| PSK | Phase Shift Keyed，相移键控 |
| PV | Primary Variable，主变量 |
| QV | Quaternary Variable，第四级变量 |
| RF | Radio Frequency，无线电频率 |
| RFD | Reduced Function Device，精简功能设备 |
| RAM | Random Access Memory，随机存取记忆体 |
| RFID | Radio-Frequency Identification，无线电频率识别 |
| RMA | Rate Monotonic Algorithm，速率单调算法 |
| RSL | Received Signal Level. The signal level（in dBm）at a receiver input terminal，接收信号水平。接收器输入端的信号电平（dBm） |
| RSSI | Received Signal Strength Indication，接收信号强度指示 |

（续）

| 名　字 | 定　义 |
|---|---|
| RTOS | Real-Time OS，实时操作系统 |
| SAP | Service Access Point，服务访问点 |
| SCADA | Supervisory Control And Data Acquisition，监控和数据采集 |
| SFD | Start of Frame Delimiter，帧首定界符开始 |
| SINR | Signal to Interference-Plus-Noise Ratio，信号与干扰加噪声比 |
| SNR | Signal to Noise Ratio，信噪比 |
| SOM | Start of the Message，报文的开始 |
| SP | Service Primitive，服务原语 |
| STX | Start of a transaction. An STX is used to convey a Network layer packet（an NPDU）from one node to an adjacent node，事务开始。STX 被来将网络层报文（NPDU）从一个节点传送至另一个相邻节点 |
| SV | Secondary Variable，次要变量 |
| TDMA | Time Division Multiple Access，时分多址 |
| TDOA | Time Difference of Arrival，到达时间差 |
| TER | Transaction Error Rate，事务错误率 |
| TCP | Transmission Control Protocol，传输控制协议 |
| TCP/IP | Transmission Control Protocol/Internet Protocol，传输控制协议/Internet 协议 |
| TPDU | Transport PDU，运输层 PDU |
| TTL | Time To Live，生存时间 |
| TV | Tertiary Variable，第三级变量 |
| UTC | Coordinated Universal Time，协调通用时间 |
| UWB | Ultra Wideband，超宽带 |
| WHA | WirelessHART Adapter，WirelessHART 适配器 |
| WHD | WirelessHART Device，WirelessHART 设备 |
| WINA | Wireless Industrial Networking Alliance，无线工业网络联盟 |
| XML | eXtensible Markup Language，可扩展标记语言 |

# 第22章　定　　义

4～20mA：点对点或点对多点的电路，主要用于过程自动化现场将工业现场中仪器和传感器的信号传输到控制器。4～20mA的模拟信号分别对应着一些过程变量的0%～100%量程。作为一种电流回路信号，4～20mA信号线也同时可以为传感器的信号收发器提供电源，并且比基于电压的信号线具有更强的抗干扰能力。

Absolute slot number（绝对时隙数）：从网络形成时开始计数的全部时隙。注：该值总是递增的，并且永远不会复位为任何固定值或零值。它的当前值始终是当前时隙的序列号，且最大值为（$2^{40}-1$）。

Acknowledge（确认）：用于对成功接收来自于DLE源设备的定向、非广播DLPDU，或者对双DLPDU通信中的第二个DLPDU成功接收的、明确的数据链路层响应。

Adapter（适配器）：对于不能直接连接到WirelessHART网络的现场设备，适配器是能与该现场设备连接并通信的网络设备。

Advertise DLPDU（通告DLPDU）：用于邀请新设备加入网络的DLPDU。注：当某个设备想加入网络时，该设备先侦听通告DLPDU，然后利用通告DLPDU中的信息来与网络同步并发起入网过程。

Analog channel（模拟信道）：将现场设备连接到数据采集端或控制系统的不断变化的电信号。注1：一些现场设备支持多个模拟输入或输出信道。注2：每个模拟信道向或从现场设备传输一个单一动态变量。

Antenna Gain（天线增益）：由天线把功率集中在某--给定方向而获得的明显功率增益。

Application（应用）：产生或使用数据的功能或数据结构。

Application layer interoperability（应用层互操作性）：应用层实体使用FAL服务实现协调和合作操作的能力。

Application object（应用对象）：穿过网络或在网络设备内，管理和提供报文交互的对象类。注：可以定义多种类型的应用对象类。

Application process（应用进程）：网络上的一部分分布式应用程序。它位于某个设备并且被明确地寻址。

Application process identifier（应用进程标识符）：区分设备中的多个应用进程。

Application process object（应用进程对象）：通过FAL应用关系能识别和访问的应用进程部件。注：应用进程对象定义由一系列类属性值组成（参见应用过程

对象类的定义)。使用 FAL 对象管理 ASE 服务可以远程访问应用进程对象定义。FAL 对象管理服务能被用于加载或更新对象定义、读对象定义、动态创建和删除应用对象及其对应的定义。

Application process object class (应用进程对象类): 依据网络可访问的属性和服务而定义的应用进程对象类。

Application relationship (应用关系): 为了交互信息和协调联合行动而在两个或多个应用实体间建立的合作关系。注: 这种关系的激活可以通过交换应用协议数据单元或者作为预配置行为的结果来实现。

Application relationship application service element (应用关系的应用服务元素): 为建立和终止所有应用关系提供唯一手段的应用服务元素。

Application relationship endpoint (应用关系端点): 应用关系中某一端应用进程观察和维护的应用关系内容和行为。注: 涉及应用关系的每个应用进程都维护自己的应用关系端点。

ASN time (绝对时隙数时间): 以绝对时隙数表示的时间。时隙内的任何时间点对应的时间都是该时隙的时隙数。

Assailant (攻击者): 产生干扰的设备。

Attribute (属性): 描述对象的外部可见特征或特色。注: 对象的属性包含了对象变量部分的相关信息。通常情况下, 它们提供状态信息或管理对象的操作。属性也可能会影响对象的行为。属性分为类属性和实例属性。

Behavior (行为): 指示对象如何响应特定的事件。注: 行为特性的描述包括属性值和服务之间的关系。

Broadcast (广播): 给所有连接到网络并能接受报文的设备发送一个 PDU 的过程。

Broadcast address (广播地址): 在有线 HART 标准中, 广播地址是主设备用于发送命令经所有设备的目标地址, 其为 38bit 长且取值全为零; 在 WirelessHART 标准中, 广播地址是将数据包同时发给所有设备时所用的目标地址, 其为 2B 长且取值为 0xFFFF。

Burst-mode device (猝发模式设备): 在没有被请求发送数据时, 一种能定期发送携带有测量数据或其他数据的设备。也就是说, 这种设备的功能像是一个独立的广播设备。猝发模式设备被定义为具有猝发能力的从设备 (因此"模式"一词被用来描述设备的类型)。当从设备中的猝发模式被启用时, 从设备被认为"处于猝发模式"。

Busy (忙): 在某个时刻忙于其他任务而不能执行当前命令的设备状态。注: 当命令规范允许时, 设备可以通过返回一个响应代码 32 表明其正处于忙的状态。

Byte (字节): 8 位, 有时候也称为 8 位位组。

**Channel（信道）**：用于发送调制信号的无线电频率带宽。

**Channel blacklisting（信道黑名单）**：屏蔽使用某信道的方法。

**Channel hopping（跳信道）**：为避免干扰和衰减而定期地、随机地改变发送或接收频率。

**Channel offset（信道偏移量）**：网络管理器提供的链路特定值，用来在跳信道时计算出实际用于通信的信道。

**Class（类）**：表示同类系统组件的一组对象。注：类是对象的泛化，也是定义变量和方法的模板。类中的所有对象在结构形式和行为特性上都是相同的，但其属性中的数据通常不相同。

**Class attributes（类属性）**：同一类中所有对象所共有的属性。

**Class code（类代码）**：分配给每个对象类的唯一标识符。

**Class specific service（类特定代码）**：由特定的对象类所定义的服务，以执行所需要的公用服务不能履行的功能。注：类特定对象对于定义它的对象类是唯一的。

**Clear channel assessment（空闲信道评估）**：当某个 RF 信道正在被占用时，对该信道进行检测以避免发起一次发送事务。注：这通过在发送事务的第 1 个 DLPDU 之前侦听该信道来实现。如果检测到信号，那么此次发送事务将被推迟稍后的某个 TDMA 时隙。

**Client（客户端）**：1）使用另一个对象（服务器）的服务来执行任务的对象。2）报文的发起方，服务器对该报文做出反应。例如，向作为服务器的单个 AR 端点发出“需证实”服务请求 APDU 的 AR 端点的角色。

**Coexistence（共存）**：当某个系统与其他相同或不同的系统共存于某个环境时，共存是指该系统在这个给定的共享环境中执行某个任务的能力。

**Connection（连接）**：与图路由有关的数据结构，其包含一对有序的网络设备。

**Conveyance path（传送路径）**：通过一个应用关系的单向 APDU 流。

**Cyclic（循环）**：用于描述重复事件的术语。

**Data-Link Layer（数据链路层）**：位于 OSI 参考模型的第 2 层。这一层负责无差错的数据通信。数据链路层定义报文结构、错误检测策略和总线仲裁规则。

**Dedicated AR（专用 AR）**：直接被 FAL 用户使用的 AR。注：在专用 AR 上，只有 FAL 头部和用户数据被传送。

**Device（设备）**：任何实现 HART 和 WirelessHART 现场总线的实体。

**Device ID（设备标识符）**：设备的序列号。注：设备制造商被要求给每个设备分配一个唯一的编号，该编号包含有设备制造商标识符和设备类型标识符。

**Device profile（设备行规）**：设备相关信息和功能的集合，为同种类型的类似设备之间提供一致性。

**Device type（设备类型）**：设备制造商的类型。注：这个属性的值是由制造商分配的。它的值指明了设备支持的命令和数据对象的集合。制造商被要求给每种类型的设备都分配一个唯一的值。例如，设备类型名就可能是其产品名。

**Device variable（设备变量）**：现场设备内唯一定义的数据项，其总是与循环的过程信息相关联。注：安装在工业过程中的设备，其设备变量值将会随着工业过程的变化而变化。

**Discovery（发现）**：通过侦听某种表明设备存在的 DLPDU 从而发现新邻居设备的过程。

**Discovery link（发现链路）**：用于发送和接收特定 DLPDU 的链路，该特定 DLPDU 能表明设备的存在。

**Dynamic variable（动态变量）**：在过程和模拟通道间的连接。注：设备可能包含主变量、第二变量、第三变量、第四变量。这些变量统称为动态变量。

**Endpoint（端点）**：一个与连接相关的通信实体。

**Error（差错）**：计算（或观察、测量）值或条件与指定（或理论）值或条件之间的差异。

**Error code（差错代码）**：在一种差错类中某个特定差错类型的标识符。

**Field device（现场设备）**：一种连接到工业过程或工厂装置的网络设备。注：现场设备直接与传感器或执行器相连，或执行过程控制功能，并且还直接连接到 HART 或 WirelessHART 的物理层。

**Frame（帧）**：数据链路层包。其包含了物理介质所需的帧头和帧尾。也就是说，网络层报文在数据链路层被封装成为帧。

**Frequency channel（频谱信道）**：在给定频率范围内频谱的划分。

**Gateway（网关）**：一种网络设备。这种网络设备包含了至少一个上位机接口（如串行口或以太网口），并充当上位机和现场设备间通信的出入口。

**Graph（图）**：一种路由结构。这种路由结构在网络设备间形成了一个定向的端到端连接。

**Graph ID（图标识符）**：用于指明某个特定图实体的标识符。

**Handheld（手持）**：便携式设备中的上位机应用程序。

**HCF enumeration（HCF 枚举）**：HART 通信基金会（HCF）控制和维护的枚举。

**Hop（跳）**：在不需要网络中其他节点参与的情况下，两个相邻节点间报文的直接传递。也用于表示改变信道的功能。

**Host（上位机）**：一个能在主设备上同时或顺序执行的应用程序。

**Interoperability（互操作性）**：互操作性是指来自于不同制造商的类似设备能协同工作于同一系统的能力，也指一个设备能在上位机系统层不丧失功能的情况下代

替另一个设备的能力。

**Join**（**加入**）：网络设备被认证并允许加入网络的过程。注：当设备拥有网络密钥、网络管理器会话、普通（非加入）超帧和链路的时候，该设备才被认为已经加入网络。

**Join key**（**加入密钥**）：用来启动加入网络过程的安全密钥。

**Latency**（**延迟**）：报文从发送方穿过网络到达接收方所花费的时间。

**Lease**（**租约**）：租赁是一种上位机和 WirelessHART 网关间在未来某段时间内共享某资源的协议。在该段时间后，该资源将会被重新分配以用于其他目的。

**Link**（**链路**）：网络中相邻设备间完整的通信规范。它包括 DLPDU 完成一跳传输所必要的通信参数。注：一个链路由源地址和目标地址对、时隙和信道偏移分配、通信方向，专用或共享通信，类型等确定。将链路分配给超帧是系统调度过程的一部分。

**Link Margin**（**链路余量**）：收到信号的功率和接收器的灵敏度之间的差异。通常情况下，它决定了某条链路的可用性。10dB 的链路余量表明该条链路是一个可靠的链路。

**Logical link control**（**逻辑链路控制**）：数据链路层两个子层中的较高层。注：该子层处理错误检测、流量控制、成帧和寻址。

**Long tag**（**长标签**）：用来标识某个现场设备的 32 字符的 Restricted ISO Latin-1 串。

**Loop current**（**回路电流**）：该值由与现场设备串联的毫安表测得。注：回路电流是近似直流的模拟（4～20）mA 的信号，用来在控制系统和现场设备之间传递单一值。当采用“回路电流”值时，电压模式的设备使用“直流电压”作为其工程单位。

**Maintenance port**（**维护端口**）：网络设备中用于预配置的接口。注：该端口可用来向网络设备写入入网密钥和网络标识符，并监测网络设备加入网络的过程。

**Management information**（**管理信息**）：网络可访问的信息，以支持管理现场总线系统的操作（包括应用层）。注：管理功能包括控制、监视和诊断。

**Manufacturer ID**（**制造商标识符**）：用来标识设备制造商的两个 8 位枚举型位组。注：制造商必须只能使用分配给自己的制造商标识符，而不允许使用分配给其他制造商的制造商标识符。

**Master**（**主设备**）：一种通过发送 APDU 请求并期待一个响应 PDU 从而启动通信活动的设备。

**Medium access control**（**介质访问控制**）：数据链路层两个子层中的较低层。注：该子层控制着对通信信道的访问。

**Multicast**（**多播**）：仅通过一次传输即可将一个报文发送给网络中的多个设备。

**Neighbor（邻居）**：网络中的相邻节点，从邻居处接收到接收信号电平（RSL）意味着至少在一个方向上通信是可能的。

**Neighbor table（邻居表）**：设备视为邻居的所有设备的列表。注：邻居表还存储有邻居的属性。

**Network（网络）**：通过某种类型的通信介质相连接在一起的一组节点。注：任何一对节点间的连接路径可能包括中继器、路由器和网关。

**Network device（网络设备）**：与网络有直接物理层连接的设备。注：每个网络设备都有唯一的用于通信的设备地址。网络设备包括现场设备、接入点（即网关）、适配器和手持。

**Network ID（网络标识符）**：一种标识符，用来标识所有设备被内连在一起的网络。注：某个网络中的某个设备无法发送 PDU 给另一个网络中的另一个设备。

**Network manager（网络管理器）**：负责配置网络、调度网络设备间通信、管理路由表、监测和报告网络健康状况的实体。注：HART 和 WirelessHART 现场总线的每个实例都只有一个网络管理器。虽然网络管理器不需要与网络有直接的物理层连接，但是它仍然需要拥有一个唯一的设备地址。

**Nickname（昵称）**：分配给网络设备的标识符，该标识符在设备所连接的网络中是唯一的。注：2 字节的昵称是由当前网络中的网络管理器来管理和分配的。

**Node（节点）**：连接到网络的可寻址的逻辑或物理设备。

**Nonce（随机数）**：为当前报文构造的唯一的不重复的数，以防止先前的通信在重放攻击中被使用。注：随机数（nonce）对于维护报文信息安全、提供发送者认证和数据报完整性方面是很有必要的。

**Omni-directional Antenna（全向天线）**：一种在所有方向都均等辐射的天线（即天线发送或接收信号的强度在所有方向都相等）。

**Packet（报文）**：在物理媒体上一次传输的按格式组合的一组比特。

**Packet Error Rate（报文错误率）**：报文被发送但是没有被正确接收到的平均数（百分比）。

**Payload data（载荷数据）**：被传输的数据报文的内容。

**Peer（对等节点）**：通信链路另一端的通信节点。通信链路终止于该通信节点里的相同协议层。

**Physical Layer（物理层）**：OSI 基本参考模型的第 1 层。物理层负责传输原始比特流、定义设备的物理（如机械、电气）连接和信号参数。

**Polling address（轮询地址）**：用于识别设备的整数。注：轮询地址用来构造一个 8 比特的地址。

**Pre-defined AR endpoint（预定义的 AR 端点）**：在设备内不通过创建（create）服务而本地定义的 AR 端点。注：那些没有预先建立的预定义 AR，在其使用前需

建立。

**Pre-established AR endpoint（预先建立的 AR 端点）**：在控制端点的 AE 配置期间，处于已建立（established）状态的 AR 端点。

**Receiver Sensitivity（接收机灵敏度）**：当 PPDU 长度为 20B 且包错误率小于 1% 时，输入信号的最小能量。

**Route ID（路由标识符）**：用来指明某个特定路由的标识符。

**Security Manager（安全管理器）**：一种应用程序，用于管理网络设备的安全资源和监控网络安全状态。

**Server（服务器）**：从通信角度，扮演 AREP 的角色。它向发起请求的客户机返回证实服务的响应 APDU。

**Server（服务器）**：从系统角度，向其他对象（客户机）提供服务的对象。

**Service（服务）**：一个对象和/或对象类根据另一个对象和/或对象类的请求而执行的操作或功能。注：定义一组公用的服务，并规定对象特定服务的定义。对象特定服务是指由特定的对象类所定义的服务，以执行公用服务不能履行的所需要的功能。

**Service Session（服务会话）**：由客户端和 WirelessHART 网关协定的服务，该服务由 WirelessHART 网关提供给客户端。

**Session ID（会话标识符）**：用于指明某个特定会话实体的标识符。

**Slave（从设备）**：从功能上分的一种设备。从设备仅在接收到来自于主设备的 PDU 请求后，才启动其通信活动，并且须对该请求做出响应。

**Slot（时隙）**：可用于相邻设备间通信的固定时间段。

**Stream（流）**：在两个应用层功能之间可靠的、虚拟的连接。对于由源设备发给其传输层的数据，流按照同样的顺序来传递该数据给目标设备。

**Superframe（超帧）**：以某恒定速率重复的一组时隙的集合。每个时隙都拥有一个与之关联的链路。

**Superframe ID（超帧标识符）**：用来指明某个特定超帧实体的标识符。

**Tag（标签）**：用于识别现场设备的长度为 8B 的 ASCII 字符串。

**Throughput（吞吐量）**：网络的有效数据传输速率。

**Time division multiple access（时分多址）**：在可能发生通信的设备间利用时隙进行媒体访问控制的技术。注：时分多址可提供无冲突的、确定性的通信。

**Time Sequence Diagram（时间序列图）**：用于阐明相同协议层之间服务关系的图表。即，对于某对对等的协议层，该协议层及其下层的协议层都被当做“黑盒子”。该时间序列图并没有显示这些协议层的内部工作方式。时间序列图展示了这些服务原语基于时间的相互作用。时间序列图有时候也被称为报文序列图。

**Timetable（时间表）**：一组参数，用来指明两个对等设备间被分配的应用程序

字段、路由和通信调度。除了与网络管理器的通信外，所有的通信都是由一个时间表控制的。

**Time to live（生存时间）**：存在于每个报文的网络层头部中的一个字段。生存时间指明了报文在被丢弃前还可以被传送的跳数。

**Transaction（事务）**：为了一个成功传输的需要，在两个对等介质访问控制实体间相关的、连续的帧交换。注：一个事务包括①源设备发出的单个 PhPDU 传输，或②在源设备发出的 PhPDU 之后，目标设备发出的数据链路层确认包 PhPDU。

**Transport Layer（传输层）**：传输层在两个设备间提供可靠的数据传输。传输层之间的通信是透明的，即不需要了解下层的传输细节。

**Unicast（单播）**：向网络中的单个设备发送一个报文。

**Unique ID（唯一标识符）**：由长度为 2B 的扩展设备类型代码和长度为 3B 的设备标识符串接而成。注：扩展设备类型代码是由 HCF（HART 通信基金会）分配的。对于用相同设备类型代码生产的每种设备，它的每个产品实现都被分配了一个唯一的设备标识符。

**UTF-8（8 位可变长度字符编码）**：UTF-8 是一种针对 Unicode 的可变长度字符编码（定长码），也是一种前缀码。

# 参 考 文 献

## HART 7.0 协议规范


1. HART Field Communication Protocol Specification (HCF_SPEC-13)
2. FSK Physical Layer Specification (HCF_SPEC-54)
3. C8PSK Physical Layer Specification (HCF_SPEC-60)
4. Wireless Physical Layer Specification (HCF_SPEC-65)
5. TDMA Data Link Layer (HCF_SPEC-75)
6. Data Link Layer Specification (HCF_SPEC-81)
7. Network Management Specification (HCF_SPEC-85)
8. Command Summary Specification (HCF_SPEC-99)
9. Universal Command Specification (HCF_SPEC-127)
10. Common Practice Command Specification (HCF_SPEC-151)
11. Wireless Command Specification (HCF_SPEC-155)
12. Device Families Command Specification (HCF_SPEC-160)
13. Temperature Device Family Specification (HCF_SPEC-160-4)
14. PID Device Family Specification (HCF_SPEC-160-7)
15. Common Tables (HCF_SPEC-183)
16. Block Data Transfer Specification (HCF_SPEC-190)
17. Discrete Applications Specification (HCF_SPEC-285)
18. Wireless Devices Specification (HCF_SPEC-290)
19. Command Specific Response Code Definitions (HCF_SPEC-307)
20. Field Device Specific Specification Template (HCF_LIT-18)
21. Field Device Specific Specification Template (Sample) (HCF_LIT-18)
22. HART Slave Data Link Layer, Test Specification (HCF_TEST-1)
23. HART Physical Layer Test Procedure (HCF_TEST-2)
24. HART Slave Application Layer Universal Command Test Specification (HCF_TEST-3)
25. Application Layer Common Practice Command Test Specification (HCF_TEST-4)


**Among these, the following specifications are new for wireless:**


Wireless Physical Layer Specification (HCF_SPEC-65)
TDMA Data Link Layer (HCF_SPEC-75)
Network Management Specification (HCF_SPEC-85)
Wireless Command Specification (HCF_SPEC-155)
Wireless Devices Specification (HCF_SPEC-290)


## HART 相关的文献

References to other standards, clarifying documents and applicable patents are listed in this subsection.


WirelessHART User Guide. HCF_LIT-84
Coexistence Test Plan. HCF_LIT-85
Approved IEEE 802.15.4 Transceivers. HCF_LIT-088

## HART 引用的相关文献

The following are applicable IEEE documents:

IEEE STD 802.15.4-2006. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs). 2006

Diffie W, Hellman M (1979) Privacy and Authentication: An Introduction to Cryptography. Proceedings of the IEEE, Vol. 67 No. 3, pp 397-427

In addition, the application of the IEEE Extended Unique Identifier (EUI-64) and Organizationally Unique Identifier (OUI) can be found at:

IEEE. (accessed 1 August, 2007). IEEE Registration Authority - Tutorials. IEEE Standards Association, http://standards.ieee.org/regauth/tutorials.html.

The following document provides additional information about and algorithms for the 16 bit ITU-T CRC (also known as CRC16).

Simpson W, Editor (1993) PPP in HDLC Framing. RFC 1549, http://www.ietf.org/rfc/rfc1549.txt, IETF 1993.

The following provides general guidelines for the specification of communication protocols.

ISO 7498-1 Information Processing Systems — OSI Reference Model — The Basic Model

On byte ordering

Wikipedia contributors (accessed 9 February, 2007) Endianness. Wikipedia, The Free Encyclopedia, http://en.wikipedia.org/w/index.php?title=Endianness&oldid=105787173.

Cohen D (accessed 9 February, 2007) On Holy Wars And A Plea For Peace, DAV's Endian FAQ http://www.rdrop.com/~cary/html/endian_faq.html.

The following reference provides additional information about and algorithms for the CCM* Mode algorithm used in conjunction with AES-128 cipher for security.

Dworkin M (2004) Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. National Institute of Standards and Technology. Special Publication 800-38C.

The following reference describes communication specification techniques.

Halsall F (1992) Data Communications, Computer Networks and Open Systems. Third Edition. Addison Wesley.

The following reference describes the methods for specifying state transition diagrams.

Hatley D. Pirbhai. I (1987) Strategies for Real-Time System Specification. Dorset House.

## 其他文献

Publications used by this book.

### Journal and Conference articles


1. Akyildiz IF. Su W. Sankarasubramaniam Y. Cayirci E (2002) A survey on sensor networks. IEEE Communication Magazine.
2. Basu A. Gao J. Mitchell JSB. Sabhnani G (2006) Distributed localization using noisy distance and angle information. MobiHOC
3. Bavier A. Feamster N. Huang M. Peterson L. Rexford J (2006) In vini veritas: realistic and controlled network experimentation. SIGCOMM. pp. 3–14. ACM.
4. Chen D. Mok AK. Baruah SK (1997) On Modeling Real-time Task Systems. Lecture Notes in Computer Science - Lectures on Embedded Systems. v(1494).
5. Chen D. Mok AK. Kuo T-W (2003) Utilization Bound Re-visited. IEEE Transactions on Computers.
6. Chen D. Nixon M. Aneweer T. Shepard R. Blevins T. McMillan G. Mok AK (2005) Similarity-based Traffic Reduction to Increase Battery Life in a Wireless Process Control Network. ISA EXPO. Chicago. USA.
7. Chen D. Nixon M. Aneweer T. Shepard R. Burr K. Mok AK (2005) Wireless Process Control Products from ISA 2004. International Workshop on Wireless and Industrial Automation.
8. Chen D. Nixon M. Aneweer T. Shepard R. Mok AK (2004) Middleware for Wireless Process Control Systems. Architectures for Cooperative Embedded Real-Time Systems Workshop.
9. Chen S. Chen Y. Trappe W (2007) Exploiting Environmental Properties for Wireless Localization. MobiCom.
10. Chung SP. Mok A (2007) Advanced Allergy Attacks: Does a Corpus Really Help? RAID. LNCS 4637. 236-255.
11. Cristian F. Fetzer C (1999) The Timed Asynchronous System Model. IEEE Transactions on Parallel and Distributed Systems. 10(6). June. 642-657.
12. Culler D. Estrin D. Srivastava M (2004) Overview of Sensor Networks. Computer.
13. Diffie W. Hellman M (March 1979) Privacy and Authentication: An Introduction to Cryptography. Proceedings of the IEEE. Vol. 67 No. 3. pp 397-427.
14. Elbatt T. Saraydar C. Ames M. Talty T (2006) Potential for Intra-Vehicle Wireless Automotive Sensor Networks. IEEE Sarnoff Symposium. pp. 1-4.
15. Elnahrawy E. Li X. Martin R (2004) The Limits of Localization Using Signal Strength: A Comparative Study. IEEE SECON.
16. Fang L. Du W. Ning P (2005) A beacon-less location discovery scheme for wireless sensor networks. Infocm.
17. Guha S. Murty RN. Sirer EG (2005) Sextant: A Unified Framework for Node and Event Localization in Sensor Networks. MobiHoc.
18. Hightower J, Boriello G (2001) Location Systems for Ubiquitous Computing. IEEE Computer. vol. 34. no. 8. pp.57–66.
19. Han S. Song J. Zhu X. Mok AK. Chen D. Nixon M. Pratt W. Gondhalekar V (2009) WiHTest: Compliance Test Suite for Diagnosing Devices in Real-Time WirelessHART Network. RTAS.
20. Hu L, Evans D (2004) Localization for Mobile Sensor Networks. MobiCom.
21. Krishnamurthy L, Adler R, Buonadonna P, Chhabra J, Flanigan M. Kushalnagar N. Nachman L, Yarvis M (2005) Design and deployment of industrial sensor networks: experiences from a semiconductor plant and the north sea. SenSys. pp. 64–75.
22. Kuo T-W. Mok AK (1991) Load Adjustment in Adaptive Real-Time Systems. IEEE Real-Time Systems Symposium.
23. Liu CL. Layland JW (1973) Scheduling Algorithms for Multiprogramming in a Hard-Real-Time Environment. Journal of ACM.
24. Liu J. Zhang Y. Zhao F (2006) Robust distributed node localization with error management. MobiHOC.

25. Liu W, Lou W, Fang Y (2005) An efficient quality of service routing algorithm for delay-sensitive applications. Computer Networks, v(47).
26. Luo J, Shukla HV, Hubaux JP (2006) Non-Interactive Location Surveying for Sensor Networks with Mobility-Differentiated ToA. INFOCOM.
27. McCluer S (2003) Wanted: Real World Battery Life Prediction. American Power Conversion Coporation.
28. Nixon M, Chen D, Blevins T, Mok AK (2008) Meeting Control Performance over a Wireless Mesh Network. CASE.
29. Nixon M, Shepard R, Bennett B, Chen D, Mok AK (2004) A Framework to Transmit Process Control Data over Commercial Wireless Networks. ISA Technical Conference.
30. Nixon M, Shepard R, Mok AK, Bennett B, Chen D (2005) Process Control Adopts Wireless. InTech Magazine, 52(2).
31. Peng C, Shen G, Zhang Y, Li Y, Tan K (2007) BeepBeep: A High Accuracy Acoustic Ranging System using COTS Mobile Devices. ACM SenSys.
32. Sha L, Rajkumar R, Lehoczky J (1990) Priority Inheritance Protocols: An Approach to Real-Time System Synchronization. IEEE Trans. on Computers, 39(9), 1175-1185.
33. Sha L, Rajkumar R, Sathaye S (1994) Generalized Rate-Monotonic Scheduling Theory: A Framework for Developing Real-Time Systems. In Proceeding of the IEEE. Vol. 82. No. 1, pp. 68-82.
34. Sheldon M, Chen D, Nixon M, Mok AK (2005) A Practical Approach to Deploy Large Scale Wireless Sensor Networks, Workshop on Resource Provisioning and Management in Sensor Networks.
35. Soldati P, Zhang H, Johansson M (2008) Deadline-constrained transmission scheduling and data evacuation in wirelessHART networks. Technical Report, Automatic Control Lab, School of Electrical Engineering, Royal Institute of Technology, Sweden.
36. Song J, Han S, Mok AK, Chen D, Lucas M, Nixon M, Pratt W (2008) Wirelesshart: Applying wireless technology in real-time industrial process control. RTAS, pp. 377–386.
37. Song J, Han S, Mok AK, Chen D, Nixon M (2007) A study of process data transmission scheduling in wireless mesh networks. ISA EXPO Technical Conference.
38. Song J, Han S, Mok AK, Chen D, Nixon M (2007) Centralized Control of Wireless Sensor Networks for Real-Time Applications, 7th IFAC International Conference on Fieldbuses and Networks in Industrial and Embedded Systems.
39. Song J, Han S, Zhu X, Mok AK, Chen D, Nixon M (2008) Demonstration of a complete wirelesshart network. SenSys demo.
40. Song J, Mok AK, Chen D, Nixon M (2006) Challenges of Wireless Control in Process Industry. Workshop on Research Directions for Security and Networking in Critical Real-Time and Embedded Systems.
41. Song J, Mok AK, Chen D, Nixon M (2006) Using Real-Time Logic Synthesis Tool to Achieve Process Control over Wireless Sensor Networks. RTCSA.
42. Song J, Mok AK, Chen D, Nixon M, Blevins T, Wojsznis W (2006) Improving pid control with unreliable communications. ISA EXPO Technical Conference.
43. Stankovic J, Lee I, Mok A, Rajkumar R (2005) Opportunities and Obligations for Physical Computing Systems. IEEE Computer, 38(11), November, 23-31.
44. Stankovic J, Spuri M, Ramamritham K, Buttazzo G (1998) Deadline Scheduling For Real-Time Systems: EDF and Related Algorithms. Kluwer Academic Publishers, Boston.
45. Thonet G, Allard-Jacquin P, Colle P (2008) ZigBee - WiFi Coexistence - White Paper and Test Report, Schneider Electric.
46. Vieira MAM, da Silva DC Jr, Coelho CN Jr, da Mata JM (2003) Survey on wireless sensor network devices. Emerging Technologies and Factory Automation.
47. Weiss JM (2005) Cyber Security Meets Plant Politics. InTech Magazine.
48. Woo H, Mok K (2007) Real-Time Monitoring of Uncertain Data Streams using Probabilistic Similarity. RTSS.
49. Zhang H, Soldati P, Johansson M (2009) Efficient Link Scheduling and Channel Hopping for Convergecast in WirelessHART Networks. Technical Report, Automatic Control Lab, School

of Electrical Engineering, Royal Institute of Technology, Sweden.
50. Zhang H, Soldati P, Johansson M (2009) Optimal Link Scheduling and Channel Assignment for Convergecast in Linear WirelessHART Networks. Technical Report, Automatic Control Lab, School of Electrical Engineering, Royal Institute of Technology, Sweden.
51. Zhu X, Dong W, Mok AK, Han S, Song J, Chen D, Nixon M (2009) A Location-determination Application in WirelessHART. RTCSA.

## Books

1. Blevins T, McMillan G, Wojsznis W, Brown M (2002) Advanced Control Unleashed: Plant Performance Management for Optimum Benefit. ISA Press.
2. Callaway EH Jr, Callaway EH (2003) Wireless Sensor Networks: Architectures and Protocols. CRC Press.
3. Caro D (2004) Wireless Networks for Industrial Automation, ISA Press.
4. Chen D (1999) Real-Time Data Management in the Distributed Environment. Ph.D. Thesis, the University of Texas at Austin.
5. Gutierrez J, Callaway E, Barrett R (Jan 1, 2007) Low-Rate Personal Area Networks: Enabling Wireless Sensors with IEEE 802.15.4. 2nd edn.
6. Halsall F (1992) Data Communications, Computer Networks and Open Systems. 3rd edn. Addison Wesley.
7. Hieb B (2003) Developing a Small Wireless Control Network. Master's Thesis, the University of Texas at Austin.

## Standards and Organizations

1. (November 2001) Advanced Encryption Standard (AES), U. S. FIPS Publication 197, DoC/NIST.
2. (1993) Automatic Controller Dynamic Specification. EnTech Control Engineering Inc., http://www.emersonprocess.com/entechcontrol/download/publications/control.pdf, Version 1.0.
3. Bluetooth. www.bluetooth.com/bluetooth
4. Electronic Device Description Language, http://www.eddl.org
5. Foundation Fieldbus, www.fieldbus.org
6. HART Foundation, www.hartcomm.org
7. IEEE 802.11 Task Group, grouper.ieee.org/groups/802/11
8. IEEE 802.15.4 WPAN Task Group, www.ieee802.org/15/pub/TG4.html
9. IEEE wireless standards, http://standards.ieee.org/wireless
10. The Instrumentation, Systems and Automation Society (ISA), www.isa.org
11. ISO 7498-1 Information Processing Systems - OSI Reference Model - The Basic Model
12. OPC Standard, www.opcfoundation.org
13. Profibus Standard, www.profibus.org
14. Wi-Fi Alliance, www.wi-fi.org
15. Wireless Industrial Networking Alliance (WINA), www.wina.org
16. ZigBee Alliance, www.zigbee.org

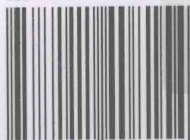
## Online documents

1. Azimuth systems inc, www.azimuthsystems.com.
2. Chipcon Products, www.chipcon.com
3. CINT, root.cern.ch/twiki/bin/view/ROOT/CINT
4. DeltaV digital control system, www.easydeltav.com
5. DEMOJM Board, www.pemicro.com/fixedlinks/demoqetoolkit.cfm
6. FreeScaleMC1321,www.freescale.com/webapp/sps/site/prod_summary.jsp?code=1321xEVK
7. FreeScale MC1322, http://www.freescale.com/webapp/sps/site/prod_summary.jsp?code=1322x_Dev_Kits&parentCode=MC13224V
8. Freescale Coldfire, www.freescale.com/coldfire
9. Robustness tester for bluetooth, www.codenomicon.com
10. ZigBee Automated Compliance Test, www.seasolve.com

# 国际视野　科技前沿

## 国际信息工程先进技术译丛

《WirelessHART：面向工业自动化的实时网状网络》
《全面的功能验证：完整的工业流程》
《无线Mesh网络架构与协议》
《UMTS蜂窝系统的QoS与QoE管理》
《半导体制造与过程控制基础》
《WCDWA原理与开发设计》
《下一代移动系统：3G/B3G》
《IMS:IP多媒体概念和服务》（原书第2版）
《下一代无线系统与网络》
《深入浅出UMTS无线网络建模、规划与自动优化：理论与实践》
《HSDPA/HSUPA技术与系统设计——第三代移动通信系统宽带无线接入》
《无线传感器及元器件：网络、设计与应用》
《印制电路板——设计、制造、装配与测试》
《IPTV与网络视频：拓展广播电视的应用范围》
《多电压CMOS电路设计》
《微电子技术原理、设计与应用》
《蜂窝网络高级规划与优化2G/2.5G/3G/…向4G的演进》
《基于蜂窝系统的IMS——融合电信领域的VoIP演进》
《无线网络中的合作原理与应用》
《移动电视：DVB-H、DMB、3G系统和富媒体应用》
《环境网络：支持下一代无线业务的多域协同网络》
《基于射频工程的UMTS空中接口设计与网络运行》
《未来UMTS的体系结构与业务平台：全IP的3G CDMA网络》
《UMTS-HSDPA系统的TCP性能》
《宽带无线通信中的空时编码》
《数字图像处理》（原书第4版）
《基于4G系统的移动服务技术》
《吉规模集成电路互连工艺及设计》
《高性能微处理器电路设计》



上架指导　工业技术／自动化

ISBN 978-7-111-40815-4　定价：80.00元